

## 1300- Do you agree with the definitions? Comments and Drafting Team Response

### Drafting Team Response:

The drafting team appreciates the comments it received in response to this question. The definitions have been reviewed and revised.

---

Name	Company	Response	Comment
Allen Klassen	Westar Energy	Yes	
Bill Wagner	Calpine	Yes	I recommend including more information regarding definitions and/or reference to definitions, at least in the FAQ's if not in the standard itself. For example include document links to the following definitions: Functional Model, Bulk Electric System Asset, Interconnection Reliability Operating Limits (IROL), NERC Policy 1.B, guidance for background checks, risk-based assessment methodology. Identifying specific definitions provides important context from which to interpret the appropriate application of the standard. Even in the event of multiple definitions, e.g., Bulk Electric System Asset, identifying the applicable definition for this standard provides the reference point from which to interpret the authors intent.
Dave Magnuson	Puget Sound Energy	Yes	“Critical Cyber Asset”– use CIPC definition “Bulk Electric System Assets” – make consistent and clarify Need further clarification of “Incident” and “Security Incident”
Dave McCoy	Great Plains Energy	Yes	
Doug Van Slyke	ATCO Electric Limited	Yes	

---

<b>Name</b>	<b>Company</b>	<b>Response</b>	<b>Comment</b>
Ed Riley and James Sample	California ISO	Yes	<p>We agree with the definitions in general, but would recommend the following changes:</p> <ol style="list-style-type: none"> <li>1. Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.</li> <li>2. Bulk Electric System Asset – Should be retitled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.</li> <li>3. Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers”, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.</li> <li>4. Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence. If the definition cannot be removed completely at least remove the second bullet as the first bullet sufficiently covers any incident. The reference to attempts in the second bullet dilutes the definition and could result in excessive reporting.</li> <li>5. Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”</li> </ol>
Francis Bradley	Canadian Electricity Association	Yes	
Gary H. Campbell	Individual	Yes	
Jack Hobbick	Consumers Energy	Yes	<p>Although we agree, the definitions are incomplete. Definition needs to be supplied for:</p> <p>Critical Cyber Information</p> <p>Large Quantities of Customers</p> <p>Extended Period of Time</p> <p>Critical Cyber Security Assets (sect 1306, para a.1)</p> <p>Critical Infrastructure (section 1306, para a.10 and 11)</p>
Jeff Schlect	Avista Corporation	Yes	

Name	Company	Response	Comment
Kurt Muehlbauer	Exelon Corporation	Yes	<p>Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operation. Exelon respectfully submits the following comments to seek clarification on the draft standard and for consideration in the final standard.</p> <p><b>Cyber Assets</b>  The association of Cyber Assets to the Bulk Electric System should occur in the definition of Critical Cyber Assets. Exelon recommends that this definition be changed to: Systems and communication networks, including hardware, software, and data.</p> <p><b>Security Incident</b>  Section 1307 references the term cyber security incident. Exelon requests that the drafting team formally define the term cyber security incident or change the term being defined from security incident to cyber security incident.</p>
Mark Kuras	MAAC	Yes	
Michael Allgeier	LCRA	Yes	
Michael R. Anderson	Midwest ISO	Yes	
Neil Phinney	Georgia Transmission Corp / GSOC	Yes	<p>Cyber Assets - the definition is too vague and gives the impression that all equipment associated with SCADA falls under this definition, while examples were given in the Frequently Asked Questions document that could exclude RTU's that do not use routable protocols (Sec. 1304, questions 1 &amp; 3). A more clear definition of what "cyber" represents is in order. If "cyber" represents TCP/IP access (internet, hackers, viruses, etc), then the focus of the standard becomes more clear, as does an effort to define exactly what is a critical cyber asset.</p>
Neil Shockey	Southern California Edison	Yes	
Peggy Ladd and Linda Nappier	Ameren	Yes	
Peter Burke on behalf of ATC's Dave Mueller	American Transmission Company	Yes	

Name	Company	Response	Comment
Phil Sobol	SPP CIPWG	Yes	<p>Bulk Electric System Asset: Any facility or combination of facilities that, if unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, or would have a detrimental impact to the reliability or operability of the electric grid, or would cause significant risk to public health and safety.</p> <p>How many wiggle words do we need in the definition? Are all of the NERC standards this vague? How can one ever comply with such a subjective standard? I should probably be thankful for some vagarity (is that a word?), but the definition is unusable and should include some metrics that can be used to apply the definition. It is understood that 1300 does not extend to nuclear facilities. However, this is never really said in the Standard. We believe nuclear facilities should be noted as exempted from the Standard. This exemption could be included in the description of critical assets. - How about some guidance on what needs to be protected at substations and how to protect them? Keep wording the same. In some places you use “calendar years” and others you use just “years”. Pick one.</p>
Russell Robertson and Mitchell Needham	Tennessee Valley Authority - Transmission	Yes	The FAQ is an excellent idea. The definitions seem to match pretty well with accepted industry practice, but might still bear further review based on comments received.
Seiki Harada	BC Hydro	Yes	<p>Some of these standards are dependent upon definitions or glossaries developed elsewhere by the NERC committees. For example, “bulk electric system” and “Interconnection Reliability Operating Limit” are defined outside CIPC (The NERC Critical Infrastructure Protection Committee). The NERC members must realize that any shift in the definitions outside CIPS may undermine the original intent of the Cyber Security Standards, with no wording changes to the Cyber Security Standards. Hence any shift in definitions should be cross-checked with interpretations in all standards in which the terms appear.</p>
Shelly Bell	San Diego Gas and Electric	Yes	
Victor Limongelli	Guidance Software, Inc.	Yes	

Name	Company	Response	Comment
A. Ralph Rufrano	NYP&A	No	<p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Al Cooley	Verano, Inc.	No	
Allan Berman	LIPA	No	<p>Critical Cyber Assets:</p> <p>Comment: Is this meant to include off-site, stand-alone emergency systems such as an Alternate Control Center?</p> <p>Incident:</p> <p>Comment: Suggest modifying the definition of "Incident" as follows because the proposed definition is too broad.</p> <p>"Incident: Any physical or cyber event that:</p> <p>?disrupts the functional operation of a critical cyber asset</p> <p>?compromises the electronic or physical security perimeters."</p>

Name	Company	Response	Comment
Charles Yeung	Southwest Power Pool	No	<p>Critical Cyber Assets: Some cyber systems that would not normally be defined as critical cyber assets contribute to the critical data or decision making processes of a critical cyber asset. Likewise, some systems that would not normally be defined as critical cyber assets generate reliability data and may use a critical cyber asset to transmit that data for use by another organization's critical cyber asset for reliability purposes. For example, a RTO market system routinely calculates generation deployment instructions on a regular periodic basis (perhaps 15 minutes). The deployment instructions are sent to generation authorities for use as unit set points. Some RTO market systems calculate a net scheduled interchange value and transmit that data via ICCP (a critical cyber asset) to the balancing authority for inclusion in ACE calculation and regulation control. Compromise of the market system could theoretically result in invalid information being used in reliability operations with resulting consequences. The definition needs to clarify to what extent such systems would come under the umbrella of this standard.</p>
Charlie Salamone	NSTAR	No	<p>Incident: The following definition is from SANS  The term 'incident' refers to an adverse event in an information system and/or network or the treat of the occurrence of such an event. Incident implies harm or the attempt to harm.  Examples:  <ul style="list-style-type: none"> <li>• Unauthorized use of another user's account</li> <li>• Unauthorized use of system privileges</li> <li>• Execution of malicious code that destroys data</li> </ul> </p> <p>Event:  An "event" is any observable occurrence in a system and/or network  Examples  <ul style="list-style-type: none"> <li>• A system crash</li> <li>• Packet flooding within a network</li> <li>• The system boot sequence.</li> </ul> </p> <p>Critical Cyber Assets - Use definition from CIPC</p> <p>Bulk Electric System Assets - define large quantity of customers</p>

Name	Company	Response	Comment
Christopher L. De Graffenried	NYP&A	No	<p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Craig Kilpatrick	Alabama Electric Cooperative, Inc.	No	<p>Bulk Electric System Asset - It my understanding that this will be changed to Bulk Electric System Facility. In either case, the definition is not very clear and could have a broad and inconsistent interpretation. Define significant impact, large quantities of customers, extended period of time, detrimental impact, and significant risk. These definitions would significantly clarify the meaning of Bulk Electric System Facility. If you want a clear understanding and a consistent interpretation this needs significant work. A clear definition should not be subject to varying interpretations.</p>

Name	Company	Response	Comment
Dave Little and Bonnie Dickson	Nova Scotia Power Inc.	No	<p>NSPI does not agree with definition in 1302.a.1. and recommends that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NSPI recommends that the definition of Critical Cyber Assets be; Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>The Incident definition should be changed from  Incident: Any physical or cyber event that: disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or compromises, or was an attempt to compromise, the electronic or physical security perimeters.  to  Incident: Any physical or cyber event that: disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset.</p>



Name	Company	Response	Comment
Dave Norton	Entergy Transmission	No	<p>Definition of “Critical Cyber Assets”: On Page 3, the first paragraph of 1301 Security Management Controls addresses "Critical business and operational functions." If the definition of critical cyber assets is to include business as well as reliability functions then the definition on Page 1 should be expanded. It now only includes reliability functions. No reservation, scheduling, OASIS-type communications, or billing is mentioned in the definition. It can be argued with validity that reliable operation of the bulk power system is critically dependent upon the ability to forecast loads, hence transitively so are OASIS-type communications critical. How shall this apparent incongruity be handled? A response that OASIS is NAESB’s domain and outside that of NERC’s is not acceptable, that is, if the goal to protect the bulk power system is both serious and intended to accrue in reality. This situation needs to be addressed cooperatively to resolution by NERC and NAESB, or perhaps FERC should provide clarity concerning this matter. #Definition of “Significant Impact”: As stated, the definition of critical bulk electric system assets can readily lead to the conclusion that everything is critical, which presumably is not the intent. Accordingly, the definition needs refinement in terms of scope. For example, what is “significant impact,” and what is a “large number” of customers? Concerning the general health of the bulk electric system, is “customers” even the right way to look at the problem? It’s possible to lose EMS/SCADA “control” centers and still keep the lights on for quite some time, so please offer more specific criteria for “significant impact.” # Under “Incident”: Correct misspelling and grammar and take a look at a pre-judgment bias in the language. Check that the tenses used in the language cover what was intended-did the committee want to cover present, past and what might have happened? If so, some suggested changes are: First bullet: Disrupts, disrupted, leads to disruption or could have led (not lead) to a disruption... Second bullet: compromises, compromised, or could have been an attempt to compromise</p> <p>Under “Security Incident”: There is the same problem with tenses and pre-judgments as in #10 above. If this fits the intent, perhaps the following text might be better: "Any malicious activities which are known to have caused, or suspicious activities that could have resulted in, an incident.</p>

Name	Company	Response	Comment
David Kiguel	Hydro One Networks Inc.	No	<p>Hydro One Networks Inc. (Hydro One) recommends that the definition of Critical Cyber Assets be:</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange such that the loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets." (We recommend this definition be used in 1302).</p> <p>Hydro One does not agree with the definition of Critical Bulk Electric System Assets in 1302.a.1. We recommend that NERC creates a Glossary of Definitions that the NERC Standards can reference. This Glossary should be the sole depository of definitions used by all Standards. Definitions such as this and others used in the standards are a matter that should be addressed by a definitions team/committee where input from stakeholders in the industry is obtained and final approval by the BOT is required for their usage.</p> <p>Hydro One recommends changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <ul style="list-style-type: none"> <li>• disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</li> <li>• compromises, or was an attempt to compromise, the electronic or physical security perimeters."</li> </ul> <p>to</p> <p>"Incident: Any physical or cyber event that disrupts, or could lead to a disruption of the functional operation of a critical cyber asset."</p>

Name	Company	Response	Comment
Deborah Linke	U.S. Bureau of Reclamation	No	<p>Critical Cyber Assets definition. The later part of the first sentence, "such as...at a minimum," implies that all these assets perform critical bulk electric system functions which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.</p> <p>Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets...." The idea is to be more definitive about what information should be protected pursuant to 1301(a)(2).</p> <p>Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence, "as identified in the Reliability Function table of the Standard Authorization Request for this standard," is suggested.</p> <p>The definition of critical asset in 1302(a)(2) should be clarified. For example, one of the key determinants to whether a device is considered a critical asset is whether it uses a routable protocol. At the very least, what is considered a routable protocol should be defined in the glossary. Also, the and-or boolean logic of this section is confusing. Possibly a decision tree chart would help clarify the logic.</p> <p>Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.</p> <p>Bulk Electric System Asset – Should be retitled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.</p> <p>Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers”, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.</p> <p>Incident – This definition should be consistent with existing operation reporting requirements, which are already in existence.</p> <p>Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”</p> <p>For purposes of this cyber standard, that the physical perimeter under consideration be that associated only with the cyber assets (e.g., the control room), not that associated with the physical (facility) asset. Physical asset breaches should be addressed under other guidance.</p>
Dennis Kalma	Alberta Electric System Operator	No	<p>The standard does not identify “key cyber personnel” nor contemplate any assurance measures around them. We like to see a better definition here for Incident. Should the words Major/minor be used here?</p>

Name	Company	Response	Comment
Ed Goff	Progress Energy	No	<p>Critical Cyber Assets -- should be amended to clarify these are cyber assets that would adversely impact the reliability of CRITICAL Bulk Electric Assets and include the criteria as identified in section 1302.a.2</p> <p>Bulk Electric System Asset -- definition too vague, should include more specifics such as those defined in section 1302.a.1</p>
Edward C. Stein	FirstEnergy Services	No	<p>Definition for Bulk Electric System Asset is not consistent with it's intent. This is a highlevel component that is really facility based and should be reflected as "Bulk Electric System Facility".</p> <p>There is definition or criteria stated for the Risk Assessment. There should be three definitive levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.</p> <p>Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR. Bulk Definitions need to be clear and consistent from one NERC document to the next if a true "consensus" throughout the industry is desired by NERC prior to balloting. The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers,etc. that are not networked nor communicated to in any way.</p> <p>Definitions section needs to clearly define "routable protocol" in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.</p> <p>Definitions section also needs to define "dial up accessible" for same reasons noted above.</p>
Everett Ernst	OGE Energy Corp	No	<p>The definition of Security Incident should agree with NIPC-IAW-SOP as known or suspected to be of malicious origin and it should be clarified that Standard 1300 incident reporting applies only to Security Incidents as defined.</p>

Name	Company	Response	Comment
Francis J. Flynn Jr.	National Grid, USA	No	<p>National Grid recommends that the definition of Critical Cyber Assets be;            "Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (National Grid has also recommended this verbiage be used in Section 1302).</p> <p>National Grid does not agree with the definition of Bulk Electric System Asset nor in the definition used in Section 1302.a.1. and further recommends that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>National Grid recommends changing the Incident definition from            "Incident: Any physical or cyber event that:            disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or            compromises, or was an attempt to compromise, the electronic or physical security perimeters."            to            "Incident: Any physical or cyber event that:            disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Francois Lemay	Brascan Power	No	<p>Clarify the distinction among 'incident', 'cyber incident', 'security incident', and 'cyber security incident'. Do not define these (differently) in more than one, e.g., 1302 and the definition section Clarify the distinction among 'critical bulk electric system asset', 'bulk electric system asset', and 'critical cyber asset'. Do not define these (differently) in more than one sections e.g., 1302 and the definition section</p>

Name	Company	Response	Comment
Greg Fraser	Manitoba Hydro	No	<p>Critical Cyber Assets suggest revised definiton: Cyber assets supporting a critical bulk electric system asset meeting the criteria in the cyber security standard. In the current posting, the definition and section 1302 requirements do not line up. The term critical cyber assets should refer those cyber assets to which the cyber security standard applies.</p> <p>Bulk Electric Security System Asset. Remove this definiton as it is now redundant.</p> <p>Critical Bulk Electric System Asset. Add this definition and remove the definition from section 1302 (a) to include here. It should be defined outside the body of the standard.</p> <p>Incident: Remove this definition as it will probably not be relevant in a glossary of terms which applies to all standards.</p> <p>Security incident: Should be revised to include the definition of incident to ensure that this definiton is stand alone within a glossary of terms relevant to all standards.</p>
Guy V. Zito NPCC CP9	Northeast Power Coordinating Council	No	<p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Hein Gerber	British Columbia Transmission Corporation	No	

Name	Company	Response	Comment
Howard F. Rulf	We Energies	No	<p>Recommend the following alternative definitions:            "Incident": Delete this definition.</p> <p>"Security Incident": Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset; or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.</p>
Jim Hiebert	WECC EMS WG	No	<p>Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.            Bulk Electric System Asset – Should be retitled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.            Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers”, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.            Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence.            Security Incident – This definition should read; “Any malicious or suspicious activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”</p>

Name	Company	Response	Comment
Joanne Borrell	FirstEnergy Solutions	No	<p>Definition for Bulk Electric System Asset is not consistent with its intent. This is a high level component that is facility based and should be reflected as "Bulk Electric System Facility". Definitions: Bulk Definitions need to be clear and consistent from one NERC document to the next if a true “consensus” throughout the industry is desired by NERC prior to balloting. The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.</p> <p>Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.</p> <p>Definitions section also needs to define “dial up accessible” for same reasons noted above.</p> <p>There is definition or criteria stated for the Risk Assessment. There should be three definitive levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.</p> <p>Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR.</p>



Name	Company	Response	Comment
Joe Weiss	KEMA	No	<p>Bulk Electric System Asset is defined as: “Any facility or combination of facilities that, if unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, or would have a detrimental impact to the reliability or operability of the electric grid, or would cause significant risk to public health and safety.” There are numerous distribution facilities that meet this definition. In fact, some critical distribution facilities would meet all three criteria. Since NERC’s charter does not address distribution, I recognize that NERC cannot specify distribution should be included in 1300. However, NERC should encourage responsible entities to apply the standard to additional assets that are found to be critical upon the execution of a vulnerability and risk assessment. One possible approach would be through the Frequently Asked Questions (FAQ)</p> <p>Security Incident is defined as any malicious or suspicious activities which are known to cause, or could have resulted in an incident. An incident is defined as any physical or cyber event that disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset. An unintentional event such as IT performed an unauthorized scan can, and has caused disruption of the functional operation of a critical cyber asset. Consequently, Security Incident should have the verbage "any malicious or suspicious" removed.</p>
John Lim	Con Edison	No	<p>Bulk Electric System Asset: "would have a significant impact on the ability to serve large quantities of customers for an extended period of time" and "or would cause significant risk to public health and safety" are subjective and not necessarily related to the operation of the bulk electric system. The scope of this standard should be focused on critical cyber assets affecting the reliable operation of the bulk electric system.</p>

Name	Company	Response	Comment
Karl Tammar	ISO-RTO Council	No	<p>It would be helpful to define and/or describe somewhere within the standard the industry groups, committees, and other structures frequently used and referenced. Identification of the compliance administration/monitor is not clear. Believed to be the RROs. This could be made clearer in the standard?</p> <p>Bulk Electric System Asset: For consistency, the word reliability should be used on its own and operability should be excluded. Both terms seen as the same.</p> <p>Incident: Delete second bullet. Because the first bullet sufficiently covers any incidents. "Attempt" dilutes the definition and could cause excessive reporting.</p> <p>Any malicious or suspicious activity which is known to have caused or could have resulted in an incident.</p> <p>We suggest changes to the following two definitions: Incident: Remove the second bullet because the first bullet sufficiently covers any incident. The reference to "attempt" in the second bullet dilutes the definition and could cause excessive reporting.</p> <p>Security Incident: Should read - Any malicious or suspicious activity which is known to have caused or could have resulted in an incident.</p>
Kathleen M. Goodman	ISO New England Inc.	No	<p>Comments Bulk Electric System Asset – There are too many different definitions being used by various groups. BES should not be defined in a cyber security standard. It should make reference to a standard definition provided elsewhere. The lack of one standard definition elsewhere does not justify it here. NERC must address this.</p> <p>The use of the term "attempt" in the basic incident description implies "malicious activity." Suggest rewording as follows: Incident: Any physical or cyber event that disrupts or compromises the functional operation of a critical cyber asset and/or the security perimeters. Security Incident: Any malicious or suspicious activity that is known to have caused an incident.</p>

Name	Company	Response	Comment
Kenneth A. Goldsmith	Alliant Energy	No	<p>Bulk electric system facility and critical cyber assets included in this section are further defined in 1302. Suggest defining once and providing further explanation in the FAQ.</p> <p>The definitions for critical bulk electric system facility and critical cyber asset are not clear. Establishing some additional criteria such as generation over 500 mw and transmission over 230 kv would be valuable.</p> <p>Remove the separate definition of an Incident and have this standard include only Security Incident. The definition should remove 'could have resulted in' as this is too subjective.</p> <p>Define Personnel and remove from 1302.</p> <p>Include IROL definition and remove from 1302.</p>

Name	Company	Response	Comment
L.W. Brown	EEI Security Committee	No	<p>Even if terms are not defined in this section, they need to be used with greater consistency, including the use of only one term to represent one concept. For example: are there intentional differences among “key staff,” “employee,” and “personnel”? If so, why, and what are those differences?</p> <p>“Critical Cyber Assets” –</p> <p>Use the CIPC-approved definition – using a different one creates confusion (not to mention wasteful duplication of effort).</p> <p>It should be explicitly clarified that the term “telemetry” does not include “telecommunications” equipment in general.</p> <p>“Bulk Electric System Assets” –</p> <p>There needs to be one single industry definition, but it ought not to be located here. Rather, it should be part of another NERC standard.</p> <p>What is meant by the term “large quantities of customers”? If it cannot be defined, it should be addressed in the FAQ, referring to the IAW-SOP definition.</p> <p>“Incident” &amp; “Security Incident” – The original language is inadequate/inappropriate for usage in subsect.1307, especially regarding the reporting of all “incidents.” Merge the two definitions into a single definition one for “Security Incident”:</p> <p>Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset, or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.</p> <p>Reference throughout is made to “compliance monitor” without definition. Who is this intended to be – employee or independent contractor?</p> <p>Add subsection (a)(1)(ii) from Section 1302.</p>

Name	Company	Response	Comment
Larry Conrad	Cinergy	No	<p>Definitions need to be clear and consistent from one NERC document to the next if a true “consensus” throughout the industry is desired by NERC prior to balloting. Because documents such as Version 0 glossary, Standard 1300, and the Risk Assessment are all being developed simultaneously, it is difficult to get a consistent understanding of what participants are being asked to agree to. Examples include but are not limited to (1) Version 0 seems to have a different interpretation of Bulk Electric System than the way it is used in Standard 1300 (2) Risk Based assessment document, part of the criteria to identify the critical cyber assets, is not yet published (3) Version 0 defines a “Reportable Disturbance” as subject to regional interpretation. Cinergy believes such a regional interpretation will be problematic for Standard 1300 language. The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. Cinergy seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.</p> <p>Definitions section needs to clearly define “routable protocol” in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.</p> <p>Definitions section also needs to define “dial up accessible” for same reasons noted above.</p>

Name	Company	Response	Comment
Laurent Webber	Western Area Power Administration	No	<p>Critical Cyber Assets definition. The later part of the first sentence, "such as...at a minimum," implies that all these assets perform critical bulk electric system functions which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.</p> <p>The definition of Critical Bulk Electric System assets in 1302 should also be modified by eliminating item (ii), item (B) under (iv), and item (vi). Including substation equipment in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assessment) as needed.</p> <p>Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets...." The idea is to be more definitive about what information should be protected pursuant to 1301(a)(2).</p> <p>For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpreted differently by each entity.</p> <p>For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This will be interpreted by each individual entity and may result in thousands of reports daily.</p> <p>For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague and would be interpreted differently by each entity.</p> <p>Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence, "as identified in the Reliability Function table of the Standard Authorization Request for this standard," is suggested.</p> <p>The definition of critical asset in 1302(a)(2) should be clarified. For example, one of the key determinants to whether a device is considered a critical asset is whether it uses a routable protocol. At the very least, what is considered a routable protocol should be defined in the glossary. Also, the and-or Boolean logic of this section is confusing. Possibly a decision tree chart would help clarify the logic.</p>

Name	Company	Response	Comment
Linda Campbell	FRCC	No	<p>The definition of critical cyber assets should be reworded to clearly indicate that it includes only those facilities that would impact the ability to operate the bulk electric system. Where there are plant and transmission facilities that can be operated without the associated cyber assets, those cyber assets should not be considered “critical” cyber assets.</p> <p>The definition of physical security boundaries should not be assumed to be a room. It should take into account that a cage or cabinet (which provides physical security and may be inside a computer room or other room) may be the boundary inside which critical cyber assets are stored.</p> <p>Definition of security incident should be more specific. Any network scan or probe could be interpreted as an activity that “could have resulted” in an incident and these occur too frequently across the industry to have a manageable process if all were reported. We recommend dropping the phrase “or could have resulted” from this definition.</p> <p>Add definitions in this section for Deviations, Exemptions, and Exceptions clearly stating the difference between these terms (if there is any) and how they apply to compliance reporting, i.e. are you fully compliant if you have an exemption from a standard? If all terms are intended to convey the same thing, use only one term in all subsequent sections. For instance, in section 1301 the use of the terms “exception, deviation and exemption” is inconsistent and what they are deviations to/from (requirements or policy) varies:</p> <p>Requirements (a) (1) (3) – “deviations or exceptions from the requirements of this standard”</p> <p>Measures (b) (1) – says “maintain documentation of” (iii) / “review all” (iv) “deviations or exemptions”</p> <p>Compliance Monitoring Process (d) (3) (iii) - documentation of justification of deviations or exemptions</p> <p>Levels of non-compliance – (e) (1) (iii) and (e) (3) (ii) “deviations to policy “</p>

Name	Company	Response	Comment
Lloyd Linke	WAPA	No	<p>Critical Cyber Assets definition. The later part of the first sentence "such as...at a minimum" implies that all these assets perform critical bulk electric system functions, which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.</p> <p>The definition of Critical Bulk Electric System assets in 1302 should also be modified, by eliminating item ii), item B) under iv), and item vi). Including substation equipment in a blanket fashion for the industry in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assesment) as they believe it is needed/justified.</p> <p>Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets...". The idea is to be more definitive about what information should be protected pursuant to 1301 (a)(2).</p> <p>For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpreted differently by each entity.</p> <p>For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This would be interpreted differently by each individual entity and may result in thousands of reports daily.</p> <p>For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague, and would be interpreted differently by each entity.</p> <p>For the definition of "Responsible Entity" - since definitions are to be included in a separate glossary, rewording the last part of the sentence "as identified in the Reliability Function table of the Standard Authorization Request for this standard" is suggested.</p>



<b>Name</b>	<b>Company</b>	<b>Response</b>	<b>Comment</b>
Lyman Schaeffer	Pacific Gas & Electric	No	<p>efinitions (Page 1):</p> <p>The definition of Critical Cyber Assets includes the term “telemetry.” Does this include all of our telecom/network assets or is this limited to the telemetry devices within the substation. This is repeated elsewhere in the document and specifically on page 9. We have been led to believe that it is the later but clarification would be very helpful.</p> <p>While we are not troubled by the definition of an incident as “any physical or cyber event that disrupts or could have led to disruption of the functional operation of a critical cyber asset,” we are very concerned that there is an apparent requirement in Section 1307 to document, investigate, and analyze all such incidents which, as defined, in very broad and potentially includes every momentary ICCP failure, EMS fail-over, and other relatively common occurrences. Our analysis indicates that we could be documenting, investigating, and analyzing literally hundreds of such incidents each year which would be onerous for us and of little practical value to the Electricity Sector ISAC. We believe that the more logical requirement would be to report only incidents that are severe or extended in duration or where we have reason to suspect that they are malicious in nature.</p>
Michael Pyle	Entergy Nuclear	No	This subject is broad enough that additional definitions will be required.
Michael R. Anderson	Midwest ISO	No	

Name	Company	Response	Comment
Paul McClay	Tampa Electric Company	No	<p>The definition of critical cyber assets should be reworded to clearly indicate that it includes only those facilities that would impact the ability to operate the bulk electric system. Where there are plant and transmission facilities that can be operated without the associated cyber assets, those cyber assets should not be considered “critical” cyber assets.</p> <p>The definition of physical security boundaries should not be assumed to be a room. It should take into account that a cage or cabinet (which provides physical security and may be inside a computer room or other room) may be the boundary inside which critical cyber assets are stored.</p> <p>Definition of security incident should be more specific. Any network scan or probe could be interpreted as an activity that “could have resulted” in an incident and these occur too frequently across the industry to have a manageable process if all were reported. We recommend dropping the phrase “or could have resulted” from this definition.</p> <p>Add definitions in this section for Deviations, Exemptions, and Exceptions clearly stating the difference between these terms (if there is any) and how they apply to compliance reporting, i.e. are you fully compliant if you have an exemption from a standard? If all terms are intended to convey the same thing, use only one term in all subsequent sections. For instance, in section 1301 the use of the terms “exception, deviation and exemption” is inconsistent and what they are deviations to/from (requirements or policy) varies:  Requirements (a) (1) (3) – “deviations or exceptions from the requirements of this standard”  Measures (b) (1) – says “maintain documentation of” (iii) / “review all” (iv) “deviations or exemptions”  Compliance Monitoring Process (d) (3) (iii) - documentation of justification of deviations or exemptions  Levels of non-compliance – (e) (1) (iii) and (e) (3) (ii) “deviations to policy “</p>
Pete Henderson	IMO	No	<p>The definition of “Incident” should be revised by deleting the second bullet. The first bullet sufficiently covers any incident.</p> <p>The definition of “Security Incident” should read, ‘Any malicious or suspicious activity which is known to have caused, or could have resulted in, an incident’.</p> <p>The standard often refers to industry groups, committees and other structures. It would be helpful to have these defined and/or described somewhere within the standard.</p>

Name	Company	Response	Comment
R. Scott McCoy	Xcel Energy	No	<p>Critical Cyber Assets definition. The later part of the first sentence "such as...at a minimum" implies that all these assets perform critical bulk electric system functions, which is not consistent with criteria in 1302 (for example, small generators). Removing it is recommended since specifics are addressed in 1302.</p> <p>The definition of Critical Bulk Electric System assets in 1302 should also be modified, by eliminating item ii), item B) under iv), and item vi. Including substation equipment in this standard is not workable for numerous reasons. NERC should establish a cyber security standard that will advance the cause of security AND be workable to implement. Substation equipment should be captured by utilities under item vii (risk-based assesment) as needed.</p> <p>Need to include definitions of the terms: Owners, Custodians, and Users. It would be a good idea to include a definition of "Sensitive Information" or something similar that refers to "information pertaining to critical cyber assets...". The idea is to be more definitive about what information should be protected pursuant to 1301 (a)(2).</p> <p>For the definition of Incident, recommend the phrase "or could have lead to a disruption of" be removed. How would one measure/determine if it "could have" lead to a disruption? It would be interpreted differently by each entity.</p> <p>For the definition of Incident, the phrase "or was an attempt to compromise" should be eliminated. This will be interpreted by each individual entity and may result in thousands of reports daily.</p> <p>For the definition of Security Incident, recommend the phrases "are known to" and "or could have resulted in" be removed. They are vague, and would be interpreted differently by each entity.</p> <p>Responsible Entity. Since definitions are to be included in a separate glossary, rewording the last part of the sentence "as identified in the Reliability Function table of the Standard Authorization Request for this standard" is suggested.</p>

Name	Company	Response	Comment
Ray Morella	FirstEnergy Corp	No	<p>Definition for Bulk Electric System Asset is not consistent with it's intent. This is a highlevel component that is really facility based and should be reflected as "Bulk Electric System Facility".</p> <p>There is definition or criteria stated for the Risk Assessment. There should be three definitive levels for the risk assessment starting at the top with Bulk Electric System Facility, then Critical Cyber Assets (System Functions) and Cyber Assets. This should be spelled out in the standard and not added as a FAQ.</p> <p>Applicability: Should contain a disclaimer that the NUKES are not included, currently if you want that information you have to go to the SAR. Definitions Section</p> <p>Page 1</p> <p>The definition of "Cyber Assets" (on page 1 of the draft) is vague and leaves room for interpretation, and how it is interpreted could have drastic impact. The term "cyber" in the heading implies computerized equipment, particularly that which can be networked together via electronic communications, however the definition does not specifically state that. ABC seeks clarification from NERC regarding "non-computer" devices such as protective relays, solid-state transducers, etc. that are not networked nor communicated to in any way.</p> <p>Definitions section needs to clearly define "routable protocol" in the definitions including what is a routable protocol and what is not a routable protocol. While the definition may be familiar to many, this concept is key to identifying the critical cyber assets, yet no definition is provided.</p> <p>Definitions section also needs to define "dial up accessible" for same reasons noted above.</p>

Name	Company	Response	Comment
Raymond A'Brial	Central Hudson Gas and Electric Corp.	No	<p>CHGE's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>Under Bulk Electric System Asset what is meant by large quantities of customers. tandard needs to have one single industry definition.</p> <p>Incident and Security Incident - Inadequate for usage in subsect. 1307</p> <p>CHGE's participating members recommend changing the Incident definition from</p> <p>Additional terms may need to be added - Even if terms are not defined, they needs to be used with greater consistency, and consistent terms need to be chosemn. For example: there are intentional differences amoung key staff, employee and personnel.</p> <p>CHGE's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p>

Name	Company	Response	Comment
Richard Engelbrecht	Rochester Gas and Electric	No	<p>RGE also concurs with the following NPCC comments:</p> <p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>

Name	Company	Response	Comment
Richard Kafka	Potomac Electric Power Company	No	<p>While the definition section offers some clarity, it is not entirely clear what is in scope and out of scope for this standard. Clarification with some of the existing definitions is needed (e.g. Bulk Electric System Asset and Critical Cyber Assets) to help with the understanding of what is in scope. Additional definitions are required for terminology utilized in the standard which are not presently defined under the definitions (e.g. Under Control of a Common System, Compliance Monitor, Routable Protocol, differentiation between Special Protection Scheme and a standard Protection System.). In some cases the definition is provided within the standard or FAQ rather than in the definition section (e.g. Section 1302.a.1.ii). In some cases there are inconsistencies in the standard (e.g. Section 1306.b.2 and Section 1301.a.5.iv.) where a definition might offer consistency. Definition: The definition of Responsible Entity needs clarification (e.g. Is all generation included? Excluded?). Section 1301.a.3 (Page 3) uses Responsible Entity and the present definition does not assist in understanding this section. Definition: Other terms used in the standard should also be defined. Such terms include Routable Protocol, Dial-up access point (local vs. remote), differentiation between a Special Protection System and a Standard Protection System. Definition: Recommend utilizing the CIPC definition of Critical Cyber Assets. Definition: There is a need for a single industry definition for Bulk Electric System Assets and Critical Bulk Electric System Assets. What is meant by large quantities of customers or significant impact or risk? Perhaps the IAW-SOP definition in the FAQs should be utilized or referenced. Definition: Clarity is needed between the definitions of Incident and Security Incident. Recommend removing the definition of Incident and clarify the definition for Security Incident. (e.g. Security Incident: Any malicious act or suspicious event that compromises or was an attempt to compromise the electronic or physical security perimeter of a critical cyber asset; or, disrupts or was an attempt to disrupt the operation of a critical cyber asset.) Definition: Clarity is needed on the dial-up perimeter definition. Does it only include the modem or does it also include the device providing password security? If a device dials a critical cyber asset is the device in scope?</p> <p>Definition: Even if terms are not defined, there is a need for terms to be used consistently (e.g. Are there intentional differences among “key staff,” “employee,” and “personnel?”).</p>

Name	Company	Response	Comment
Robert E. Strauss	New York State Electric and Gas Corp.	No	<p>NYSEG concurs with the following NPCC comment:</p> <p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>



Name	Company	Response	Comment
Robert Pellegrini	United Illuminating	No	<p>NPCC's participating members recommend that the definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or</p> <p>compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that:</p> <p>disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Robert V. Snow P.E.	Robert Snow	No	<p>The definition of the bulk electruc system should include a voltage definition similar to previous NERC definitions. The typical is to define systems equal to or greater than 100 kV. An additional description are systems that are contained in a FERC tariff for jurisdictional entities or as defined in the applicable documents for others.</p> <p>Add a new definition for intrusion Assessment. It is an analysis by an independent entity that attempts to defeat the security systems being defined. It is a standard practice in the cyber industry and other parte of the electric utility industry.</p>

Name	Company	Response	Comment
Roman Carter	Southern Company	No	<ul style="list-style-type: none"> <li>• The definition of 'Bulk Electric System Asset' includes statements such as 'affecting the ability to serve customers or risk to public health and safety'. However, FAQ #4 asks why those terms were left out of the standard and then provides a reasonable explanation as to why they were left out, but they are still in the standard.</li> <li>• The definition of 'Critical Cyber Assets' does not mention that the asset must use a routable protocol or be dial-up accessible, which is a major point and needs to be mentioned in the definition. Consider adding clarification that the asset must be remotely controllable as well. If the asset uses the routable protocol or modem for read purposes only it should not be considered a critical cyber asset.</li> <li>• The definition of 'Incident' and 'Security Incident' use terms such as 'could have led' or 'could have resulted in'. The standard can not be considered 'crisp' if basic definitions are based on what might could happen and not what did happen.</li> <li>• The definition of 'Incident' includes 'was an attempt to compromise the electronic perimeter'. Script kiddies and compromised hosts on the Internet 'attempt to compromise the electronic perimeter' thousands of times per day. Need more clarity here as to the intent, which I assume is a 'targeted attack' and not just the usual Internet noise. Applicability • This standard only references its application to Functional Model entities and omits NERC itself. By virtue of NERC sponsoring and/or operating computer systems such as the Interchange Distribution Calculator (IDC) and other mechanism such as System Data eXchange (SDX), Reliability Coordinator Information System (RCIS), and NERCnet/ISN it has access to reliability information that must be protected per 1301(a)(2). In addition, the NERC-sponsored IDC through its receipt of Tag data and its implementation of TLR requests would seem to be subject to 1302(a)(1)(i)(A) as a Critical Bulk Electric System Asset due to its activities of "monitoring and control", "real-time power system modeling", and "real-time inter-utility data exchange."</li> <li>• Add – "function" to the end of the sentence after "Entity"</li> </ul>

Name	Company	Response	Comment
S. Kennedy Fell	New York Independent System Operator	No	<p>The NYISO recommends that the definition of Critical Cyber Assets be;          "Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>The NYISO does not agree with definition in 1302.a.1. The NYISO supports the idea of having a stand alone definitions document to accompany the entire set of standards. The NYISO also recommends changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that:          disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or          compromises, or was an attempt to compromise, the electronic or physical security perimeters."          to</p> <p>"Incident: Any physical or cyber event that:          disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>
Stacy Bresler	PacifiCorp	No	<p>Bulk Electric System Asset/Facility" – seriously needs clarification, as this definition is used to include/exclude assets. In particular, we need quantification around the terms "significant", "large", "extended", and "significant risk". Definitions Bulk Electric System Asset/Facility" – seriously needs clarification, as this definition is used to include/exclude assets. In particular, we need quantification around the terms "significant", "large", "extended", and "significant risk".</p> <p>Definitions Incident: Any physical or cyber event that: ..." – define "event" and define "could" as used in the next two bullet points. Without clarification, we must be inundated with events because every virus event, every internet attack "could" (if we failed to configure things correctly) cause a problem.</p> <p>Incident: Any physical or cyber event that: ..." – define "event" and define "could" as used in the next two bullet points. Without clarification, we must be inundated with events because every virus event, every internet attack "could" (if we failed to configure things correctly) cause a problem.</p>

Name	Company	Response	Comment
Terry Doern	Bonneville Power Administration	No	<p>2. Bulk Electric System Asset – The term “if unavailable” narrows the applicability of the standard to that portion of “Bulk Electric System Assets” that are somehow made unavailable AND have “a significant impact on the ability to serve large quantities of customers for an extended period of time” etc. If the definition applies to a loss of “availability”, then “Incidents” must correlate to such loss. This is standard cyber security practice. Also, the terms “significant impact”, “large quantities”, “detrimental impact” and “significant risk” are not defined.</p> <p>3. Electronic Security Perimeter – The statement “and for which access is controlled” narrows the definition of the perimeter to networks that have access control in place. If no access control is in place, then they would be outside the security perimeter. If the intent of the standard is to bring uncontrolled networks into best practice compliance, then this definition is counterproductive. This statement should be changed to “and for which access should be controlled”.</p> <p>4. Physical Security Perimeter – As with the comment for the definition of Electronic Security Perimeter, the statement “and for which access is controlled” should be changed to “and for which access should be controlled”.</p> <p>5. Incident – The terms Physical and cyber event” should be dealt with separately. With reference to these events, the terms “could have” and “an attempt to” are counter to cyber security industry practice. These terms are impossible to correlate to any criteria and are not reportable. An incident should be a concrete benchmark related to actual activity and not intentions.</p> <p>The terms “disruption” and “compromise” are not defined...They should be clearly defined as an impact, such as a disruption which led to a loss of availability of a critical bulk electrical system asset or a compromise which sent out confidential data. As a federal agency, BPA has been given criteria for reportable security incidents.</p> <p>6. Security Incident – The terms “malicious” and “suspicious” are nebulous and not defined. Delete them from this definition.</p> <p>7. Definitions need to be provided for the terms: Bulk Electric System Asset and Critical Bulk Electrical System Assets.</p> <p>BPA Transmission is in agreement with the following WECC EMS WG’s comments:</p> <p>8. Critical Cyber Assets – The term “adversely impact” needs to be defined more clearly.</p> <p>9. Bulk Electric System Asset – Should be retiled as “Critical Bulk Electric System Asset” and the definition should be defined by the NERC Operating Committee.</p> <p>10. Bulk Electric System Asset – The terms “significant impact”, “large quantities of customers”, “extended period of time”, “detrimental impact”, and “significant risk” all need to be clearly defined.</p> <p>11. Incident – This definition should be removed based on existing operation reporting requirements, which are already in existence.</p> <p>12. Security Incident – This definition should read; “Any malicious or suspicious</p>

Name	Company	Response	Comment
Tom Flowers	CenterPoint Energy	No	activity which is known to have caused or would have resulted in an outage or loss of control of a Critical Cyber and/or Critical Bulk Electric Asset.”
			Replace the current definition of “Critical Cyber Assets” with ... “Those [Cyber] facilities, systems, and equipment which, if destroyed, damaged, degraded, or otherwise rendered unavailable, would have a significant impact on the ability to serve large quantities of customers for an extended period of time, would have a detrimental impact on the reliability or operability of the electric grid, or would cause significant risk to public health and safety. For the purposes of this Standard, the following critical Cyber assets are not addressed: (1) critical telecommunication infrastructure, (2) critical RTUs, PLCs, or Meters other than where specifically included, (3) critical Cyber support infrastructure, (state other exceptions and exclusions here)”
			Delete the definition of “Incident”
			Replace the definition of “Security Incident” with... “Any malicious or suspicious activity that has or could disrupt or compromise critical Cyber assets or its support infrastructure.”
Tom Pruitt	Duke Power Company	No	Insert definitions for: common systems, authorized access, unauthorized access, contractors or vendors, employees or staff, compliance audit, large quantity of customers (ESISAC website #s), (a thorough search and review of needed definition is needed)
			There is some confusion and need for clarity on some of the terms. See comments in the details section of the accompanying document.
Tony Eddleman	Nebraska Public Power District	No	Vague wording is used throughout the standard. How do we know if we are compliant with the standard? The openness of the standard is good from the perspective that it allows each entity to apply the standard to their situation, but will make compliance difficult. An individual entity may consider they are compliant, but actually not be compliant with the standard. Some examples are:

Name	Company	Response	Comment
William J. Smith	Allegheny Energy	No	<p>Cyber Asset - The definition does not specify computer assets, which could be interpreted to include non-cyber assets such as motor control centers or physical switches that could be defined as hardware.</p> <p>Critical Cyber Assets - The definition should be standardized with other NERC documents and within the document itself. The criteria for identifying critical cyber assets (Section 1302.a.2) should be part of the definition.</p> <p>Physical Security Perimeter - Reword the definition to address networks that are not confined to a specific area or room, such as power station control networks that may exist throughout a power station and connect to devices directly on the plant floor and not in a room.</p> <p>Incident and Security Incident should be combined into one definition that addresses security incidents only. Wording such as "could have lead to a disruption" and "could have resulted in" should be revised to read "disrupts, or could have directly resulted in a disruption" and "could have directly resulted in" respectively.</p> <p>Also, the Security Incident definition should be specific enough to insure activities such as "denied access" card reads are not condidered a suspicious activity.</p>

## Do you believe this standard is ready to go to ballot?

Name	Company	Response	Comment	Drafting Team Response
Bill Wagner	Calpine	Yes	I agree with the Requirements and Measures sections. There are several editorial errors (e.g., erroneous list numberings), and the Compliance Monitoring and Levels of Noncompliance sections are very different between all of the sections. This makes for a very awkward if not impractical standard to actually audit and enforce. Standardize the Compliance Monitoring and Levels of Noncompliance subsections. For example, Section 1304 Electronic Security has a very straight forward approach for Compliance Monitoring and Levels of Noncompliance. Note, this may require revising the individual "Measures" sections to ensure the proper documentation is required/created such that it can be monitored.	The drafting team will review the compliance monitoring and levels of noncompliance sections for consistency.

Name	Company	Response	Comment	Drafting Team Response
Dave McCoy	Great Plains Energy	Yes	<p>Comment 1. Reference to specific line items throughout the standard uses inconsistent formats. In 1302 under the provision for Critical Cyber Assets in item E) a reference is made to 1302.1.2.1. I believe this is referring to 1302 (a) (2) (i). It would make more sense to change to format of the standard to the numerical format for consistency.</p> <p>Comment 2. Your FAQ's are great and perhaps this question could be addressed in an addition to this list. Please give examples of what is anticipated in terms of risk-based assessments. These are referred to in several places and it would be helpful to know if this is load flow studies or something else.</p> <p>Comment 3. The Compliance Monitoring Process appears to be almost identical in each standard. Perhaps at least a portion of it could be stated in a separate standard and not repeated eight times.</p> <p>Comment 4. A Compliance Schedule is needed for SAR 1300. It should state that compliance should not take effect until the certification in the first quarter of 2007. This is necessary, because most NERC members have already developed their 2005 budgets, and it would be very difficult to pursue compliance before 2006. SAR 1200 should continue to rule in the interim.</p> <p>Comment 5. No compliance matrix was included with SAR 1300. This should be added, even though presumably it is the same table that was included with SAR 1200.</p> <p>Comment 6. It would be helpful to have a requirement timetable matrix that lists all of the compliance requirements along with each one's respective periodicity.</p>	<p>Formatting will be corrected.</p> <p>FAQs will be updated to address risk assessment.</p> <p>Compliance monitoring criteria are required for each section.</p> <p>A draft implementation plan will be posted with the draft version 2 of this standard. A compliance matrix will accompany the final draft standard.</p> <p>The drafting team will consider developing a timetable matrix as a separate reference document.</p>



Name	Company	Response	Comment	Drafting Team Response
Neil Shockey	Southern California Edison	Yes	The "Applicability" section on page 2 should be revised to explicitly exclude nuclear units from the standard as they fall under NRC jurisdiction. In addition, the timelines throughout the standard need to be reconciled as there are variations in the time allotted to cancel electronic/physical access following termination, suspension, transfer, etc.	<p>The exclusion of nuclear units will be addressed in the standard's applicability section.</p> <p>Timeframe references will be reviewed for consistency, but are necessary for measuring compliance.</p>
Peggy Ladd and Linda Nappier	Ameren	Yes		
Peter Burke on behalf of ATC's Dave Mueller	American Transmission Company	Yes		
Russell Robertson and Mitchell Needham	Tennessee Valley Authority - Transmission	Yes	This is a guarded 'yes'. There have been a number of comments pertaining to clarification of a 'critical' asset. In addition, there does appear to be an inconsistent approach to the various sections of each article, something which could lead to differing interpretations among entities. It would be difficult to agree with the standards as presently written, but would be considered given the importance of this issue.	The standard will be reviewed for clarity.

Name	Company	Response	Comment	Drafting Team Response
A. Ralph Rufrano	NYPA	No	<p>As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.</p> <p>NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".</p> <p>Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p>	<p>A draft implementation plan will be posted with draft version 2.0 of this standard.</p> <p>The standard will be reviewed for clarity and consistency.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p>
Al Cooley	Verano, Inc.	No		
Allan Berman	LIPA	No		

Name	Company	Response	Comment	Drafting Team Response
Allen Klassen	Westar Energy	No	<p>Reconsider the clarification of requirements of the increased scope of 1300 vs 1200. Please do NOT use an existing NERC Policy i.e. Policy 1.B as a reference to define a requirement.</p> <p>Pick a value, such as 800 Mws, or define the requirement directly in this standard. Reference to a document that is planned to be obsolete and does not address cyber security only adds confusion to the interpretation of this standard.</p>	Section 1302 will be reviewed for clarity.
Charles Yeung	Southwest Power Pool	No	<p>General comment: Southwest Power Pool participated in drafting of comments submitted by the ISO-RTO Council and concurs with all comments in that filing. In those comments, the ISO-RTO Council recognizes certain members may have additional comments that would be filed individually. We submit these comments in addition to the ISO-RTO Council filing as they are specific to SPP's opinions and do not believe they conflict with the ISO-RTO Council comments.</p> <p>General comment: Standard needs to use consistent terminology. For example, the standard refers to the following terms, all assumed to be equivalent: "critical information," "critical cyber information," and "critical cyber asset information."</p> <p>General comment: References to periods of time should be clarified to indicate whether the time reference is clock/calendar hours/days or business days. For example, does 1301 (b) (5) (i) Access Authorization refer to 5 calendar days or 5 business days? Likewise, does the reference in 1301 (b) (6) to 48 hours refer to 2 calendar days or 2 business days?</p>	Terminology and time references will be reviewed for consistency and clarity.

Name	Company	Response	Comment	Drafting Team Response
Charlie Salamone	NSTAR	No	Needs to be more specific around RTUs. This is provided in the FAQs; why not bring into the standard.  Format of how standard is written; inconsistent (i.e. numbering throughout the standards document)	RTUs are examples of cyber assets and the drafting team does not believe they should be singled out.  The standard will be reformatted.

Name	Company	Response	Comment	Drafting Team Response
Christopher L. De Graffenried	NYPA	No	<p>NPCC's participating members feel there is much redrafting to be done to the standard and that the following items may be considered "show stoppers" by some.</p> <p>Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue. NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.</p> <p>As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.</p> <p>NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".</p> <p>Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated</p>	<p>Definitions will be reconsidered in light of the comments received.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p> <p>The drafting team will review the compliance monitoring and levels of noncompliance sections for consistency with the requirements.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>Section 1303 will be reviewed.</p> <p>References will be corrected.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p> <p>NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>The references within the standard made to other portions of Standard 1300 are not correct. Without clear references, NPCC cannot determine if the document is acceptable or not. For example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Each one of these incorrect references must be corrected.</p>	

Name	Company	Response	Comment	Drafting Team Response
Craig Kilpatrick	Alabama Electric Cooperative, Inc.	No	<p>There is typically one control center per bulk transmission service area and this will require a redundant or backup facility. Are you saying that you must have a backup control center? or Are you saying you must have redundant systems and/or a backup control center?</p> <p>In the Webcast that NERC hosted 10/18/04, we were asked to provide input in regards to implementation of 1300. Will compliance be based on a point in time (snapshot) or is it dependent on a continual basis? Computer systems that log transaction related to electronic access and physical access are subject to failure and down-time related to maintenance. Without having all of these systems in some sort of failover redundant mode, no one can ensure that all transactions would be captured. Would compliance be nullified if a logging PCs disk crashed and had to be repaired in order to recover the logging function? If safeguards are in place to document failures or gaps in data is this enough? I believe that compliance will be very difficult for everyone if you do not have a snapshot provision or allowances for application failure. Implementation of compliance deadlines should be related to the time that the standard is implemented. Due to the broadening of the scope in regards to areas that are applicable, current plans based on UAS-1200 will require a significant rework. Full compliance with 1300 should be atleast 1 full year from the date of issuance and preferrably at the first of a calendar year. Assuming adoption in 2005 and to allow for budget cycles, I would suggest compliance January/2007 with a snapshot provision. Allow for compliance with UAS-1200 for January/2006.</p>	<p>This standard does not require a backup control center.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard and will recognize a phased-in approach to compliance.</p>

Name	Company	Response	Comment	Drafting Team Response
Dave Little and Bonnie Dickson	Nova Scotia Power Inc.	No	<p>We have reviewed the proposed 1300 standard and would like to start by complimenting the Standards Development Team for their hard work and for the professional product they have produced. We have also worked with our CEA (Canadian Electricity Association) and its members; and our NPCC associations/teams to create joint comments on this proposed standard for submission. We would, however, like to take this opportunity to directly comment on this proposed standard on behalf of our company. In this portion of our submission, we would like to make directional comments on this proposed standard and its implementation.</p> <p>The first comment really speaks at the grass roots of this standard and how it should be interpreted and/or implemented. Our industry is composed of companies that have very little in common except our product. Our location, our size, our construction, our position and impact on the grid all differentiate us one from another. The concept of singular standards is viable but the "across the board" application of them will not be a success without introducing the concept of variable risk. We believe that it is the responsibility of each entity to implement its own risk assessments (cyber/physical/HR) based on a continuum of risk that includes factors like geopolitical location/risks, architecture of infrastructure/systems/operations, and the impact that cyber/physical events can have on the bulk power systems, our customers and public good. We believe that these risk assessments are the domain of the responsible entity and should be the singular driving force to the application of all policies and standards including the NERC 1300 Standard. We, along with many of our industry partners, believe that standards should be implemented in accordance with an entity's real risks. This means that all measures; cyber, physical and human resource are to be subjugated to an entity's risk assessment. The phrase "in accordance with an entity's risk assessments" is notably absent in your standards and yet, ultimately,</p>	<p>The draft standard refers to risk assessment in Section 1302.</p> <p>Definitions will be reconsidered in light of the comments received.</p> <p>The drafting team will review the compliance monitoring and levels of noncompliance sections for consistency with the requirements.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p> <p>Section 1303 will be reviewed.</p>



Name	Company	Response	Comment	Drafting Team Response
			<p>key to its success.</p> <p>The second topic echoes many of the comments we have heard both directly from our associates but also over and over in your Web Conference in October. We are referring to the issues and continual discussions with regards to the definitions included in this proposed standard. The industry's preoccupation with these definitions just echoes how critical they are to the interpretation and eventual success of this standard. We endorse the concept of centralized definitions that this standard and others would depend upon to function. The creation of clear, concise centralized definitions would provide the bedrock upon which these and other standards could solidly be understood and applied. Standard 1300 is based on the definition of critical BES assets , (defined in 1302.a.1). Per question 1, we do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue. Also we feel the need to change the Incident definition as shown in Question 1 is important.</p> <p>Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and</p>	

Name	Company	Response	Comment	Drafting Team Response
			<p>posted with the next posting of this Standard.</p> <p>We are in general agreement with the intent of Section 1303, however a prescriptive approach to be applied to all entities regardless of size, geography etc. is not reasonable. Responsible entities should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>The term -background screening- has too many issues, we recommend that this section's title become - Personnel Risk Assessment-.</p> <p>As noted in previous comments NSPI supports the NERC decision to move away from monetary sanctions.</p> <p>We would also like to express our concern over the significant incremental administrative tasks and documentation requirements to be compliant with this standard and hope the Standard Drafting Team will consider this during the development of the associated Implementation Plan.</p>	
Dave Magnuson	Puget Sound Energy	No		

Name	Company	Response	Comment	Drafting Team Response
Dave Norton	Entergy Transmission	No	<p>1. General Comment - Publishing a security plan is a security risk. Similarly, publicly issuing minimum cyber security standards may pose additional risk to those who want to be protected by the standards, and may pose an opportunity to those seeking to intrude. Would be intruders would already know the minimum baseline for protections by just reading about the measures required by NERC in 1300. Given the expense of any security plan in terms of bureaucracy and cost, potential intruders may logically assume that measures beyond those required by NERC would not be taken, making it easier for him or her to overcome the published barriers. Moreover, should a potential intruder access some of the required plans, documentation, records and reports called for in the plan, such documents would make it easier for the intruder to cause mischief. In the absence of such required documentation, the potential intruder would likely encounter a consistent degree of chaos from company to company. In summary, it is neither a wise nor common practice for any organization seeking a certain level of security to publish what its comfort zone consists of. Should the NERC Cyber Security Standard 1300 be confidential, not public?</p> <p>2. General Comment - The investigation, clearing functions, personnel training, tracing, tracking, reporting and record keeping requirements of the proposed standards are onerous. It isn't the practice of standards settings groups to estimate the cost and manpower required to comply with new requirements, however, it seems that the consumer, who has no vote in the standards-making process but will ultimately cover the cost in rates or fees, should be considered as a new security bureaucracy is proposed. Cost and manpower estimates should be considered in the interest of the ratepayers and regulators.</p> <p>3. General Comment - The intent and purpose and the desired objective of the standards should be more clearly defined. Just reducing risk seems passive and</p>	<p>NERC's ANSI-accredited standards development process requires public posting of its standards.</p> <p>The drafting team recognizes the potential impacts and has made every effort to minimize the burden while fulfilling the goal of this standard.</p> <p>The purpose section will be redrafted.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard. A compliance matrix will be available when the standard is posted for ballot.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>narrow in scope. On the proactive side we could be raising barriers as well. "Reducing risk" is indeterminate in the methods of interference that could be tackled. For instance, bogus phone calls could cause havoc, but such human interactions, devoid of cyber or physical penetration are not addressed.</p> <p>4. General Comment - OASIS postings are required by Order 889. The Cyber Security standard does not mention OASIS, or OASIS postings specifically. It does, however, require we "post" info (page 34). All Transmission Providers (TPs) under FERC jurisdiction provide information via OASIS on their transmission system to the public. They also provide additional information to certificated entities and people. The relationship between Order 889 and the Cyber Security standards should be addressed and clarified. An example of a potential conflict is that in drawing a perimeter around "Cyber Assets" and "Critical Cyber Assets," which are described to include X, Y and Z "at a minimum" it is possible that TPs will consider or should consider that some of the functions, information, load flow cases, and postings on OASIS should be considered "cyber assets that perform critical bulk electric system functions"</p> <p>5. General Comment – Sanctions: There are no definitive sanctions outlined in the draft standard. Does this mean there still will be no official "teeth" enabling NERC to collect penalties? 12. Page 2: Effective Period Definition - With the stroke of a pen by the NERC Board of Trustees 1300 becomes instantly in effect, with no allowances for implementation realities. There needs to provisions allowing for phased implementation. Even the toughest state regulators make allowances for a phase in of their reliability regulations (e.g., Texas PUC Substantive Rule 25.52). Without some accounting for the difficulty and expense of implementing required changes, in some situations it may drive "check the box" behavior rather than engender a smart implementation, when the smart implementation takes more time. Binary, instantaneous</p>	

Name	Company	Response	Comment	Drafting Team Response
			<p>compliance requirements do not appear to be the best way to drive corporate behavior to achieve the desired results. Provisions for a phased implementation should be embraced in earnest.</p>	

Name	Company	Response	Comment	Drafting Team Response
David Kiguel	Hydro One Networks Inc.	No	<p>The items listed below are what Hydro One would consider show stoppers in the balloting of the Standard.</p> <p>Standard 1300 is based on what are the critical BES assets, which is defined in 1302.a.1. As stated in our response to question 1, Hydro One does not agree with that definition and have made suggestions as to what may the Drafting Team may do to address the issue.</p> <p>Hydro One believes that the concept of the Bulk Electric System and associated "definitions" used in the development of the Standard may not be appropriate to capture its intent. We suggest substantive changes as shown in question 3. We strongly believe that the Standard is to be based on the the concept of "Critical Functions and Tasks" that relate to the inter-connected transmission system. Each Responsible Entity should then define and use a Risk Assessment approach to:</p> <ul style="list-style-type: none"> <li>(a) identify Critical BES facilities;</li> <li>(b) identify what Cyber Assets are located within those BES facilities; and</li> <li>(c) identify what assets in (b) are critical.</li> </ul> <p>The Risk Assessment approach should be based on the degree of degradation in the performance of critical BES operating tasks.</p> <p>We also feel the need to change the Incident definition as shown in Question 1 is important.</p> <p>The references made within the Standard to other portions of 1300 are not correct. Without clear references, it is not possible to decide whether the document is acceptable or not. For example, 1301.a.3 says "as identified and classified in section 1.2." Where is this section? Every one of these incorrect references needs to be corrected.</p> <p>Throughout the document, the Compliance levels should be updated to measure revisions we suggest below.</p>	<p>Definitions will be reconsidered in light of the comments received.</p> <p>References will be corrected.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p> <p>The drafting team will review the compliance monitoring and levels of noncompliance sections for consistency with the requirements.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>Section 1303 will be reviewed in light of comments received.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>There should be a statement in the Standard that reflects:</p> <ul style="list-style-type: none"> <li>(a) all applicable confidentiality agreements obligations;</li> <li>(b) entity's disclosure of information policies; and</li> <li>(c) regulatory and legal obligations regarding Confidential Information.</li> </ul> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard 1200. In order to assess the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. This should be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p> <p>While we agree with the intent of Section 1303, the use of the term "background screening" however has too many issues and we recommend that this section's title become "Personnel Risk Assessment." Portions of 1303 are too prescriptive and our position is that that the responsible entity should have more latitude in determining what is an acceptable level of risk. We have made recommendations later in the comment form that will make this Section acceptable.</p> <p>As previously discussed and submitted with our comments to other standards, Hydro One supports NERC decision to move away from monetary sanctions, and would like to again emphatically state that Hydro One does not support monetary sanctions.</p> <p>Hydro One is also concerned about the incremental administrative tasks, documentation requirements and capital expenditures that may be required to support compliance with the 1300 standard. We expect the Drafting Team will consider the associated costs</p>	

Name	Company	Response	Comment	Drafting Team Response
			during the development of the associated Implementation Plan.	
Deborah Linke	U.S. Bureau of Reclamation	No	NERC should consider following the NIST guidance for security controls, plans, and reviews. This wouldn't cover the penalties component of the NERC materials, but it would standardize the front-end security program controls. Specific NIST guidance that would be reasonable to cite would be Special Publications 800-18 (Security Plans), 800-30 (Risk Assessments), 800-37 (Certification and Accreditation), and 800-53 (Recommended Security Controls).	The drafting team considered the NIST security publications during the development of this standard.
Dennis Kalma	Alberta Electric System Operator	No		
Doug Van Slyke	ATCO Electric Limited	No	There are a number of areas that need more detail or a supporting "intent" document is required to understand what the requirements are. In some cases you have to read the Q&A document to understand the policy.	The standard drafting team will clarify the intent.
Ed Goff	Progress Energy	No	Not knowing the proposed Implementation Plan, this standard has extended it's scope too broad as a next step beyond the existing 1200 Urgent Action Standard and would be difficult to be ratified and in place at the time the 1200 Urgent Action Standard expires in August 2005. Compliance Monitoring Process should be more focused on reviewing only the exception and change products not the complete documentation for a particular measure.  The initial documentation and ongoing documentation control/maintenance burden imposed by this standard appears to far exceed the effort required to implement and execute actual security practices. The level of documentation required under 1200 should be sufficient. The focus appears to direct entities to concentrate more on audit accountability through excessive documentation versus channeling effort to perform actual security process improvements.	A draft implementation plan will be posted with draft version 2 of this standard.  Compliance Monitoring is based on required measures, not exceptions.  The amount of documentation required in the 1300 Standard reflects the wider scope and depth of detail outlined in 1300.



Name	Company	Response	Comment	Drafting Team Response
Ed Riley and James Sample	California ISO	No	<p>The term Reliability Authority was recently removed in the creation of the NERC Standard 0. Should be reflected in the Applicability section. For consistency, the word reliability should be used on it's own and operability should be excluded. Both terms seem to be used synonymous within the standard.</p> <p>Due to formatting inconsistency, it is difficult to differentiate between the section introduction paragraph, requirements, and measurements sections. In many cases they each seem to define requirements.</p> <p>In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.</p> <p>Identification of the compliance administration/monitoring is not clear. Believed to be the RRO's. Who is responsible for overseeing compliance should be made clearer in the standard.</p> <p>The compliance section is very difficult to understand. Multiple compliance levels are complex and should just be that you are compliant or non-compliant.</p> <p>It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.</p> <p>Consider removing all timeframe references (e.g. quarterly, annually, etc.) and replace with "to ensure compliance with the entities document processes." This would achieve the goal of ensuring that the entity documents their processes and procedures and would provide them the flexibility to define their own auditable/measurable business rules.</p> <p>The standard makes heavy use and references to industry groups, committees, and other acronyms and it would be helpful to have these defined and/or described.</p>	<p>The standard will be revised to reflect the change in terminology.</p> <p>Formatting will be corrected.</p> <p>All sections will be reviewed for consistency and clarity.</p> <p>The compliance monitor is defined within the context of NERC's compliance program.</p> <p>NERC's compliance program has established the four-tiered non-compliance model.</p> <p>A compliance matrix will be available when the standard is posted for ballot.</p> <p>The drafting team believes that the diversity of entities and their business processes defines the need for minimum acceptable timeframes.</p> <p>Acronymns will be defined.</p> <p>The drafting team believes that SAS 70 control objectives go far beyond what is required in this standard.</p>

Name	Company	Response	Comment	Drafting Team Response
------	---------	----------	---------	------------------------

Due to the fact that many entities that will be required to be compliant with this standard is also subject to other regulations such as Sarbannes-Oxly (SOX). To comply with SOX many organizations are undergoing SAS 70 audits. It is highly suggested that the NERC 1300 Drafting Team try to align of control objectives within the standard with the SAS 70, both from a wording standpoint as well as an activity standpoint, to enable entities to optimize their activities as it relates to compliance and oversight.

Format inconsistencies exist throughout the document between each section. These inconsistencies results in difficulty in determining what the true requirements are. In several instances, more than one section calls for the same requirement with different time periods. The document needs a professional tech writer to review and make each section consistent and homogenous. It is understandable that the drafting team cannot provide this level of review and consideration must strongly be given to hiring a professional tech writer prior to the next publication.

Name	Company	Response	Comment	Drafting Team Response
Edward C. Stein	FirstEnergy Services	No	<p>By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).</p> <p>During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an "isolated" test environment was required. NERC Responses clearly stated that an "isolated" test environment was NOT required. This led to misunderstandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ's to embellish the requirements. Documents, such as the FAQ's, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ's.</p> <p>ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.</p> <p>ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.</p> <p>General Question If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.</p>	<p>The drafting team does not believe, nor do industry comments support the opinion that the requirements of this standard will inhibit adoption of new technology.</p> <p>The FAQs will be incorporated into the requirements to the extent possible.</p> <p>The amount of documentation required in the 1300 Standard reflects the wider scope and depth of detail outlined in 1300.</p> <p>Cost-benefit evaluation is part of each entity's risk assessment process.</p> <p>No.</p>
Everett Ernst	OGE Energy Corp	No	<p>The standard as it is written is too prescriptive, does not make provisions for legacy equipment capability, and requires too much documentation and logging.</p>	<p>The drafting team will take these comments into consideration.</p>

Name	Company	Response	Comment	Drafting Team Response
Francis Bradley	Canadian Electricity Association	No		
Francis J. Flynn Jr.	National Grid, USA	No	<p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is National Grid's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p>	<p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p>
Francois Lemay	Brascan Power	No	Numbering and not based on popular or international standards, definitions, reporting	Formatting will be corrected.

Name	Company	Response	Comment	Drafting Team Response
Gary H. Campbell	Individual	No	<p>Each requirement seems to take a different approach to the content and flow of the document. The team needs to specify and be aware of how the content of the three sections (requirements, measures and compliance levels) are to be developed and interrelate and maintain the approach throughout the standards. I believe the "requirements" section set the minimum at least or define what is acceptable, the "measures" section tell me what to go and look for and "levels of compliance" section tell me the degree of severity for not having the requirements met. The authors of these requirements in some cases intertwined these three area, especially the requirements and measures sections. In some of the requirements section, it is used as an introductory section explaining what is meant by a specific term presented.</p> <p>Compliance Monitor - CM</p> <p>Compliance Monitoring Process: In the keeping of audit records by the Compliance Monitor, it should be defined as to what records are to be kept (completed audit reports). The vague statement of keeping audit records may lead some to think they should retain the documentation observed which could lead to additional security problems.</p> <p>Measures and levels of compliance need to be explicitly defined. By that I mean to be definitive: do not use vague terms or assume the reader knows what you are talking about. Tell the reader exactly how a plan is to be defined, what is to be in the content of the requirement etc.</p>	<p>The document will be reviewed for consistency and clarity.</p> <p>The standard does not require the compliance monitor to retain documentation it reviews during the audit.</p> <p>Compliance levels will be reviewed for clarity and consistency.</p>

<b>Name</b>	<b>Company</b>	<b>Response</b>	<b>Comment</b>	<b>Drafting Team Response</b>
Greg Fraser	Manitoba Hydro	No	<p>Specific measures should appear consistently in either or both the requirements and measures subsections. The problem is that sometimes a group of text is repeated throughout a section in its various subsections but there are differences from subsection to subsection. The text may appear in the introductory paragraphs, Requirements subsection, and/or Measures subsection. Ideally the idea should be defined in only one location, and then subsequent subsections should merely refer back to it. Not only does this approach remove confusion, it also allows for more straightforward editing of the standard.</p>	The standard will be reviewed for clarity and consistency.

Name	Company	Response	Comment	Drafting Team Response
Guy V. Zito NPCC CP9	Northeast Power Coordinating Council	No	<p>As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p> <p>As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.</p> <p>NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".</p>	<p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p>
Hein Gerber	British Columbia Transmission Corporation	No		
Howard F. Rulf	We Energies	No	Cyber Security Standard 1300 should be dealing with Cyber Security Incidents only.	Definitions will be clarified.
Jeff Schlect	Avista Corporation	No		

Name	Company	Response	Comment	Drafting Team Response
Jim Hiebert	WECC EMS WG	No	<p>The term Reliability Authority was recently removed in the creation of the NERC Standard 0. Should be reflected here.</p> <p>In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.</p> <p>The compliance section is very difficult to understand. Multiple compliance levels are complex and should just be that you are compliant or non-compliant.</p> <p>It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.</p> <p>Consider removing all timeframe references (e.g. quarterly, annually, etc.) and replace with: to ensure compliance with the entities document processes. This would achieve the goal of ensuring that the entity documents their processes and procedures and would provide them the flexibility to define their own auditable/measurable business</p>	<p>The standard will be revised to reflect this change in terminology.</p> <p>All sections will be reviewed for consistency and clarity.</p> <p>NERC's compliance program has established the four-tiered non-compliance model.</p> <p>The drafting team believes that the diversity of entities and their business processes defines the need for minimum acceptable timeframes.</p>



Name	Company	Response	Comment	Drafting Team Response
Joanne Borrell	FirstEnergy Solutions	No	<p>By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).</p> <p>During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an "isolated" test environment was required. NERC Responses clearly stated that an "isolated" test environment was NOT required. This led to mis-understandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ's to embellish the requirements. Documents, such as the FAQ's, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ's.</p> <p>ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.</p> <p>ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.</p> <p>General Question</p> <p>If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.</p>	<p>The drafting team does not believe, nor do industry comments support the opinion that the requirements of this standard will inhibit adoption of new technology.</p> <p>The FAQs will be incorporated into the requirements to the extent possible.</p> <p>Amount of documentation required in the 1300 Standard reflects the wider scope and depth of detail outlined in 1300.</p> <p>Cost-benefit evaluation is part of each entity's risk assessment process.</p> <p>No.</p>

Name	Company	Response	Comment	Drafting Team Response
Joe Weiss	KEMA	No	<p>Security policies should acknowledge and consider the unique requirements of control systems. There are significant portions of traditional IT security policies that apply to control systems. However, there are other portions of traditional IT security policies that may not adequately address control system-unique issues. NERC 1300 is meant to address critical cyber assets (control systems). It has been documented that inadequate control system policies and procedures have led to many control system denial-of-service events. These events would not have been mitigated using traditional IT security policies and procedures. ISA SP99 Technical Report 2 should be explicitly referenced as it has been developed specifically for process control system security. Additionally, requirements for awareness and training should be expanded to include control system cyber security awareness and training.</p> <p>Wireless security for control system applications has not been included. Wireless security was specifically identified in the Final Report of the Northeast Blackout. Additionally, telecom security as it impacts control system operation also has not been included. Telecom issues have impacted critical control systems operations (eg, as documented by NERC, control centers, substations, and power plant operations were significantly impacted when the Slammer worm impacted frame relays, etc.).</p> <p>Access authorization should include internal employees and those non-utility employees that also require access such as control system vendors, system integrators, etc. Access authorization may not be able to be extended to control systems as the technology may not be currently available for certain plant and substation equipment.</p> <p>Requirements on Antivirus, patching, default access, etc should have a disclaimer that it be applied to the extent practical. Depending on the version and</p>	<p>SA SP99 Technical Report 2 will be referenced in the FAQs.</p> <p>Communications were omitted as a result of industry consensus during the SAR phase.</p> <p>Access control, addressing internal and third-party, is documented in Section 1304.</p> <p>Authorized exceptions are acceptable as described in 1301.</p>

Name	Company	Response	Comment	Drafting Team Response
			capability of the control system, some of these applications can actually shutdown or inhibit control system functionality.	
John Lim	Con Edison	No	The implementation of the measures, procedures and controls to provide 100% compliance can require significant efforts in manpower and investment. The implementation plan should allow for a multi-year progression towards 100% compliance without penalties.	A draft implementation plan will be posted with draft version 2 of this standard.
Karl Tammar	ISO-RTO Council	No	<p>The ISOs/RTOs have a number of regional concerns related to national, state, provincial, and local laws and requirements. General: The document could be improved through review to make each section consistent and homogeneous. Specific format inconsistencies that exist within the document are noted in the specific comments below.</p> <p>We recommend that the following general statement be added as a preamble to this standard that recognizes that this standard is to be applied in a risk management context: "This standard is intended to ensure that appropriate security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed."</p>	<p>The standard will be reviewed for consistency and clarity and will be reformatted.</p> <p>The purpose section will be revised to reflect this language.</p>

Name	Company	Response	Comment	Drafting Team Response
Kathleen M. Goodman	ISO New England Inc.	No	<p>There are too many inconsistencies in structure of the document, in the use of terms such as "monitoring", what is meant by audit data, etc. Also inconsistent between Requirements, Measures, Monitoring, and Non-compliance. The current draft requires significant clarification and re-write. This includes putting more focus on risk assessment in identifying critical BES functions and tasks, and security solutions to protect critical cyber assets.</p> <p>Identification of the compliance monitor is not clear. Is this NERC, Regional Management, or the Regional Reliability Operators. Could this be made clearer in the standard?</p> <p>3. Several references appear to "reliability" and/or "operability." Unless there is a meaningful distinction between the two, you should drop references to "operability."</p> <p>4. The 1300 standard must be very clear in that it does not mandate what department within a responsible entity is accountable for security training and/or background screening, and related records management.</p> <p>5. Compliance Monitoring -- identify specific data that is kept for three years. Need to provide clarification to indicate the meaning of audit results, which we believe means compliance with the NERC 1300 standard and not other audits. For (3)'s, please state clearly that this is to be done with respect to applicable confidentiality agreements in place. This information can be highly sensitive.</p> <p>These need to be clarified in all sections 1301 through 1308.</p>	<p>The standard will be reviewed for consistency and clarity and will be reformatted.</p> <p>The compliance monitor is defined in the context of NERC's compliance program.</p> <p>The standard will be reviewed for consistency and clarity.</p> <p>The standard does not mandate specific departmental responsibilities.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p>
Kenneth A. Goldsmith	Alliant Energy	No	<p>The standard reflects good security practices companies follow for protecting cyber assets. However, the amount of specificity within the standard cannot be applied to all assets and may not need to be applied based on risk assessments and other mitigating controls. The standard should allow exceptions and other controls within levels of compliance.</p>	<p>Authorized exceptions are acceptable as described in Section 1301.</p>

Name	Company	Response	Comment	Drafting Team Response
Kurt Muehlbauer	Exelon Corporation	No	<p>Exelon fully supports the protection of critical cyber assets that impact the reliability of the bulk electric system operation. Exelon respectfully submits the following comments to seek clarification on the draft standard and for consideration in the final standard.</p> <p>Exelon does not believe the standard is ready for ballot until the following comments are addressed. If these comments are addressed, Exelon intends to support that the standard go to ballot.</p> <p>1301 Security Management Controls</p> <p>1301.b.1.iii Please explain how deviations and exemptions impact levels of noncompliance</p> <p>1301.a.5.iv This section requires termination of user access to critical cyber assets to be accomplished within 24 hours of a change in user status. We agree that access must be updated within 24 hours for cases where a person loses his/her access rights due to cause. The NRC allows three days for a favorable termination and this standard should not be more demanding than the highly regulated nuclear industry.</p>	Section 1301 will be reviewed in light of comments received.
L.W. Brown	Edison Electric Institute	No	<p>One overarching point of great importance: If not within this standard, NERC standards in general (or at least the official, published criteria for auditing and enforcement) must have an appropriate "exceptions" policy. There will always be situations when "strict compliance" is in fact not the optimal approach for a utility or other responsible entity to follow.</p>	Authorized exceptions are acceptable as described in Section 1301.

Name	Company	Response	Comment	Drafting Team Response
Larry Conrad	Cinergy	No	<p>Definitions need to be clear and consistent from one NERC document to the next if a true "consensus" throughout the industry is desired by NERC prior to balloting. Because documents such as Version 0 glossary, Standard 1300, and the Risk Assessment are all being developed simultaneously, it is difficult to get a consistent understanding of what participants are being asked to agree to. Examples include but are not limited to (1) Version 0 seems to have a different interpretation of Bulk Electric System than the way it is used in Standard 1300</p> <p>(2) Risk Based assessment document, part of the criteria to identify the critical cyber assets, is not yet published</p> <p>(3) Version 0 defines a "Reportable Disturbance" as subject to regional interpretation. Cinergy believes such a regional interpretation will be problematic for Standard 1300 language.</p> <p>By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).</p> <p>During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an "isolated" test environment was required. NERC Responses clearly stated that an "isolated" test environment was NOT required. This led to misunderstandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ's to embellish the requirements. Documents, such as the FAQ's, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ's.</p>	<p>Definitions will be reviewed for consistency.</p> <p>Each entity is to use its own risk assessment method.</p> <p>Commentor should suggest language for a Regional Difference in Section 1302.</p> <p>The drafting team does not believe, nor do industry comments support the opinion that the requirements of this standard will inhibit adoption of new technology.</p> <p>The FAQs will be incorporated into the requirements to the extent possible.</p> <p>Amount of documentation required in the 1300 Standard reflects the wider scope and depth of detail outlined in 1300.</p> <p>Cost-benefit evaluation is part of each entity's risk assessment process.</p> <p>No.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>Cinergy is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.</p> <p>Cinergy believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.</p> <p>General Question</p> <p>If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.</p>	

Name	Company	Response	Comment	Drafting Team Response
Laurent Webber	Western Area Power Administration	No	<p>NERC should utilize existing Cyber Security standards (see series 800, Computer Security) from the National Institute of Standards and Technology (NIST) that are already well-developed, tested, and recognized by GAO, OMB, and Federal sector, instead of having electric utility people create a whole new set of such standards. Since all Federal Government agencies are currently mandated to follow the NIST guidelines, the imposition of different NERC guidelines imposes an unnecessary redundant and burdensome level of documentation and audits that result in increased cost without a commensurate improvement in security.</p> <p>In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges or if it extends to those that utilize the assets as users (dispatchers using an EMS, for example). One example of such a gray area can be found in 1301(a)(5)(ii), for example, but there are many such areas. NERC should not focus on access by those that only have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access.</p> <p>This standard is an expansion to standard 1200 and has a direct related impact on implementation and resource requirements. It would be helpful if the implementation plan were provided.</p>	<p>The drafting team considered the NIST security publications during the development of this standard.</p> <p>Access authorization applies to administrator and user. The standard will be reviewed for clarity.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard..</p>



Name	Company	Response	Comment	Drafting Team Response
Linda Campbell	FRCC	No	<p>Overall this standard is an improvement over the existing 1200 standard, especially with the inclusion of the FAQ document to assist with interpretation. However, where compliance is concerned, an organization must comply with the standard as written, and to our knowledge external documentation, such as the FAQ, is not a part of the standard. We feel that considerable work still exists to improve the wording to further clarify the standard, so that it can stand alone without the need of a FAQ for clarification.</p> <p>In addition, we have noted inconsistency and redundancy across sections of the standard, and inconsistency in some sections between requirements, measures and compliance. Often the measure is no more than a restatement of the requirement; other times it lists the requirements, where the requirement itself is vague. Non-compliance levels seem to be related to the requirements at times and at times are related to the measures. Backward references to which section of the standard non-compliance refers to might be helpful. For example in 1303, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening would be the measure. We would suggest a thorough review of requirements versus measures versus non-compliance.</p> <p>The first item of the compliance monitoring process for all sections of the standards says, "and investigations upon complaint" please clarify - "upon complaint" - of who?</p> <p>Both the standard and FAQ should be reviewed to ensure that references correspond to the proper locations within the standard document. We do not feel this standard is ready to be distributed for balloting.</p> <p>FRCC and its members recognizes that the cyber</p>	<p>The standard will be reviewed for clarity and consistency.</p> <p>Investigations are part of NERC's Compliance Program.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p>

Name	Company	Response	Comment	Drafting Team Response
			security standard has the potential to be very costly to the industry. We believe that NERC should address this cost issue in the field testing phase of any standard. Costs associated with the implementation of this standard should be fully understood as part of the standards setting process.	
Lloyd Linke	WAPA	No	<p>NERC should lean on existing standards including National Institute of Standards and Technology (NIST) Cyber Security standards (See series 800, Computer Security) that are already well-developed and tested, instead of having electric utility people create a whole new set of such standards. Also, the NERC standard seems to have redundancy with other security compliance requirements such as Sarbanes-Oxley, etc, but seems not to be well coordinated with these other standards.</p> <p>All required minimum review periods should be a standard period of one year. Having so many review periods with numerous periodicities is not practicable.</p> <p>In several places in the standard, the issue of authorized access and tracking that access is discussed. It is usually unclear if this is meant to include only those that have access with administrative privileges, or if it extends to those that utilize the assets as users (Dispatchers using an EMS, for example). One example of such a gray area can be found in 1301 (a) (5) (ii), for example - but there are many such areas. NERC should not focus on access by those that only have rights to use the system, and should clarify in all such contexts that the reference is only to those with administrative access.</p> <p>This standard is an expansion to standard 1200; implementation resource requirements look to be very significant. It would be helpful if the implementation plan were provided. Will there be an expanded implementation timeframe in which to address the standard (beyond the first quarter of 2006)?</p>	<p>The drafting team considered the NIST security publications during the development of this standard.</p> <p>Timeframes will be reviewed for consistency.</p> <p>Access authorization applies to administrator and user. The standard will be reviewed for clarity.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p>

Name	Company	Response	Comment	Drafting Team Response
Lyman Schaeffer	Pacific Gas & Electric	No	A general concern that, while the standard appears to leave discretion to the individual company to protect its assets based on its own risk assessment and other internal analysis, portions of the standard and particularly some of the compliance metrics seem to compel the implementation of certain protective measures regardless of the degree of risk or other factors.	The standard will be reviewed for consistency.
Mark Kuras	MAAC	No	Entity-level deviation and or exception from the Standard requirements should not be allowed. The only differences allowed in the Standards Process Manual are Regional Differences. This would set a precedence that could make compliance monitoring very difficult or even impossible.  Also, Distribution Providers should be subject to the requirements of the Standard and Load Serving Entities should not be subject to the requirements of the Standard.	Other comments received by the drafting team do not support this opinion.  Distribution is outside NERC's purview.
Michael Allgeier	LCRA	No	Language and flow of the Standard and fine tuning.	The standard will be reformatted.
Michael Pyle	Entergy Nuclear	No	Areas of applicability. Nuclear generators are regulated by the NRC. This standard should not attempt to place additional and possibly conflicting regulation on nuclear generators. Cutting down the sections was a good idea. Need to address regulation of nuclear generators.	The exclusion of nuclear units will be added to the applicability section.
Michael R. Anderson	Midwest ISO	No	Classification Issues – Could the Term "critical cyber assets" be clearly defined as each company will likely define these differently?	Defintions will be reconsnidered in light of the comments received.

Name	Company	Response	Comment	Drafting Team Response
Neil Phinney	Georgia trnasmission Corp / GSOC	No	<p>1302 (a)(2)</p> <p>Point 1 – The label of an asset as "critical" should be based on its function, not the communication method it uses. Use of a routable protocol may be one of several characteristics that make a device vulnerable, but it does not bear on the issue of whether a device is critical. This section even contradicts the definition in 1300 itself. The definition specifically includes devices that perform monitoring and control (presumably RTUs), but 1302 indicates that they would be included only if they use a routable protocol. Why should a device connected to a Bulk Electric System Facility be a critical asset if it uses the IP protocol to connect to the device, and not be critical if it performs the same function using a serial protocol? Whether a device is critical should depend on its function, not the protocol used or even the type of communication (dedicated or switched) to perform that function.</p> <p>Point 2 – Routable protocol networks vary dramatically and should not all be treated the same</p>	For the purposes of this standard, criticality is defined by the magnitude of vulnerability, which increases when an asset uses a routable protocol.

Name	Company	Response	Comment	Drafting Team Response
Paul McClay	Tampa Electric Company	No	<p>Overall this standard is an improvement over the existing 1200 standard, especially with the inclusion of the FAQ document to assist with interpretation. However, where compliance is concerned, an organization must comply with the standard as written, and to our knowledge external documentation, such as the FAQ, is not a part of the standard. We feel that considerable work still exists to improve the wording to further clarify the standard, so that it can stand alone without the need of a FAQ for clarification.</p> <p>The standard lacks an impact analysis (NERC &amp; market participant cost of implementation, timing, etc.). We will have to submit to the FPSC/FERC for cost recovery of the costs to implement these standards. As such NERC should include an impact analysis of implementing the new standard. We normally view the NERC standards as Regulatory requirements since compliance is essentially, mandatory. In any other venue (Nationally, Regionally or Locally) approval of a Regulatory rule is done in consideration of both an impact analysis and the public record of comments of the proposed rule. It is certainly done at FERC and it should be done in the NERC process.</p> <p>In addition, we have noted inconsistency and redundancy across sections of the standard, and inconsistency in some sections between requirements, measures and compliance. Often the measure is no more than a restatement of the requirement; other times it lists the requirements, where the requirement itself is vague. Non-compliance levels seem to be related to the requirements at times and at times are related to the measures. Backward references to which section of the standard non-compliance refers to might be helpful. For example in 1303, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening would be the measure. We</p>	<p>The standard will be reviewed for clarity, consistency, and inclusiveness.</p> <p>The drafting team recognizes the potential impact and has made every effort to minimize the burden of these requirements while fulfilling the goal of this standard.</p> <p>A draft implementation will be posted with draft version 2 of the standard.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>would suggest a thorough review of requirements versus measures versus non-compliance.</p>	
			<p>The first item of the compliance monitoring process for all sections of the standards says, "and investigations upon complaint" please clarify - "upon complaint" - of who?</p>	

Name	Company	Response	Comment	Drafting Team Response
Pete Henderson	IMO	No	<p>a. The current draft fails to properly emphasize that this standard is to be applied in a risk management context. It is therefore overly prescriptive in certain areas such as records retention durations and records revision frequencies. 1. A general statement should be made in a preamble to this standard that recognizes that this standard is to be applied in a risk management context. The following words are proposed:</p> <p>"This standard is intended to ensure that appropriate security is in place, recognizing the differing roles of each entity in the operation of the grid, the criticality and vulnerability of the assets needed to manage grid reliability, and the risks to which they are exposed.</p> <p>2. This standard includes a number of new requirements that do not appear in NERC 1200. In order to both gauge the impact of these new requirements and make viable plans to come into compliance, it is essential to understand whether it is intended to phase in implementation of the standard and the schedule for that phasing.</p> <p>3. In a number of places, the draft standard specifies that documentation is to be reviewed for accuracy and completeness within a specified time interval (sometimes annually, sometimes quarterly, sometimes every 90 days, etc). The required frequency of document review should be established by the responsible entity based on the risk associated with inaccurate or incomplete information rather than specified in terms of a prescribed time interval applicable to all responsible entities. It may be reasonable to prescribe that document review should occur no less frequently than once per year. Wording of the following form is suggested:</p> <p>The responsible entity shall update all documents in a timely fashion following the implementation of changes. Periodic reviews shall be conducted to ensure the accuracy of these documents. The responsible entity shall establish the required minimum</p>	<p>The purpose section will be revised to reflect this language.</p> <p>A draft implementation plan will be included with draft version 2 of this standard. A phased approach will be taken.</p> <p>Timeframes will be reviewed for consistency.</p> <p>Retention periods will be reviewed in light of comments received.</p> <p>The standard will be reformatted and references corrected.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>frequency of these reviews based on the risk associated with these documents being out of date or inaccurate. At a minimum, documentation shall be reviewed annually.</p> <p>If this comment is accepted, it will be necessary to revise the definitions of the various levels of non-compliance.</p> <p>4. In a number of places the draft standard specifies the length of time for which access records, firewall logs, intrusion detection logs and the like are to be retained. The retention period for logs and access records and so on should not be prescribed by this standard. Rather, retention periods should be based on the usefulness of those records at a subsequent date, the cost of retention, and the risk associated with premature deletion. That is a judgement which is best made by "the responsible entity". It is appropriate to require that required retention periods are formally documented and approved by the responsible entity.</p> <p>If this comment is accepted, it will be necessary to revise the definitions of the various levels of non-compliance. A requirement to retain logs for a longer period should a cyber security incident be detected within the normal retention period is reasonable and should be retained.</p> <p>b. Throughout the document, there are a number of inconsistencies in the way clauses are referred to, and places where clauses are referred to that do not exist. For instance, there are a number of references to 1302.1.2, yet there is no such clause. These references need to be properly correlated if the standard is to be useful.</p> <p>c. It is noted in the "Background Information" section of the Comment Form that "An implementation plan will be developed at a later date for posting with a subsequent draft of this standard". As a subsequent draft is clearly contemplated by the drafting team, balloting at this time would be inappropriate.</p>	



Name	Company	Response	Comment	Drafting Team Response
Phil Sobol	SPP CIPWG	No	<p>Consistent wording and you should be careful not to specify specific systems.</p> <p>- We do not have the staffing to implement all of these requirements. We need someone responsible for authorizing and documenting testing of changes, someone to document testing environments, someone qualified to know how to test the security of the systems, someone to test changes against security, someone to implement changes, someone to catalog and keep up with logs and records, etc. On top of that, we would have to spend all kind of money and time on test environments.</p> <p>- This standard will require some companies to restructure in order to create a security team that can work across their current department boundaries. EMS support teams, power plant control centers, substation engineers, etc, do not have the expertise to implement most of the requirements, and most IT departments do not control the software on the systems in those departments.</p>	<p>The standard will be reviewed for clarity and consistency.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard. A phased approach will be used, which is intended to help mitigate resource gaps.</p> <p>The standard does not dictate organizational design.</p>

Name	Company	Response	Comment	Drafting Team Response
R. Scott McCoy	Xcel Energy	No	<p>1302 Critical Cyber Assets, (a) (1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).</p> <p>Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station, and therefore carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?</p> <p>1302 Critical Cyber Assets, (a) (2). The logistics for Items A-E should be clarified; it is confusing.</p> <p>1302 Critical Cyber Assets, (a) (2). There should be more clarification/restatement of requirements for dial-up cyber assets</p>	<p>The language in the FAQ was excerpted from NERC Operating Policy 1B.</p> <p>The standard will be reviewed for clarity and consistency.</p>

Name	Company	Response	Comment	Drafting Team Response
Ray Morella	FirstEnergy Corp	No	<p>Definitions: Bulk Definitions need to be clear and consistent from one NERC document to the next if a true "consensus" throughout the industry is desired by NERC prior to balloting.</p> <p>By placing additional security restrictions/costs on routable (IP) technology, NERC will (in effect) slow the migration from older technologies to more flexible future technologies involving (IP).</p> <p>During the Standard 1200 process, the NERC Responses to the Ballot Comments provided a different definition than the language contained in Standard 1200 in some cases. Example: Standard 1200 clearly stated an "isolated" test environment was required. NERC Responses clearly stated that an "isolated" test environment was NOT required. This led to misunderstandings about what the real requirements were. Although the Standard 1300 process is young, there appears to be too much reliance on the FAQ's to embellish the requirements. Documents, such as the FAQ's, should be used to provide examples. The intent of the requirements should be fully explained in the Standard 1300 language, not the FAQ's.</p> <p>ABC is concerned that requirements, such as excessive documentation, will mean that resources are utilized to comply with requirements that do not truly enhance actual security.</p> <p>ABC believes that some estimate of the costs vs. the benefit of the requirements must be understood before moving toward implementation.</p> <p>General Question</p> <p>If a company goes through the process and finds that it has NO critical cyber assets, does that company have any additional obligations under Standard 1300? If so, please explain.</p>	<p>Definitions will be reviewed in light of comments received.</p> <p>The drafting team does not believe, nor do industry comments support the opinion that the requirements of this standard will inhibit adoption of new technology.</p> <p>The standard will be reviewed to clarify intent and minimize interpretation.</p> <p>Amount of documentation required in the 1300 Standard reflects the wider scope and depth of detail outlined in 1300.</p> <p>Cost-benefit evaluation is part of each entity's risk assessment process.</p> <p>No.</p>

Name	Company	Response	Comment	Drafting Team Response
Raymond A'Brial	Central Hudson Gas and Electric Corp.	No	<p>As previously discussed and commented on in various forums, CHGE supports the NERC decision to move away from monetary sanctions.</p> <p>CHGE's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated Implementation Plan.</p> <p>Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. CHGE has made some recommendations in this regard.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is CHGE's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p>	<p>A draft implementation plan will be posted with draft version 2 of this standard.</p> <p>The standard will be reviewed for clarity and consistency.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p>

Name	Company	Response	Comment	Drafting Team Response
Richard Engelbrecht	Rochester Gas and Electric	No	<p>1. In general, there are too many areas which require interpretations which are defined or included in the FAQ's. Since the FAQ's would not be part of the approval these interpretations need to somehow be included within the standard.</p> <p>2. An alternative to developing a definition of Bulk Electric System would be to require the Reliability Authority for each Control Area to identify the Bulk Electric System for its respective Control Area. The next step would be for each Responsible Entity to identify the Bulk Electric System Asset they are responsible for in that system, identify the critical operating system functions and tasks and then identify the Critical Cyber Assets.</p> <p>3. This standard is not consistent in the level of detail for each area being addressed. Also there is no process indicated for change to be made following approval. A different approach to consider would be to make the standard identifying roles and responsibilities; identification of what is required to be included within the standard and its objective; and the process for review and sanctions. A description of minimum level for each area or standard should be attached as a guideline. In that manner the Standards can be permanent and only adjust the attachment if warranted. The way the standards read now, they must be adhered to unless the responsible individual in the company grants an exemption or deviation. A standard should be a standard with no deviation. Minimum guidelines would be a more practical approach. A deviation or exemption to a guideline is a more pragmatic approach.</p>	<p>The standard will be reviewed to clarify intent and minimize interpretation.</p> <p>Definitions will be reviewed in light of comments received.</p> <p>The draft standard will be reviewed for consistency and clarity. A change process is described in NERC's Standards Process Manual.</p>

Name	Company	Response	Comment	Drafting Team Response
Richard Kafka	Potomac Electric Power Company	No	<p>The first draft of Standard 1300 is a good start in helping to focus cyber security beyond EMS/SCADA systems. Certainly a standard is needed across the industry. However we believe that there are significant issues that need to be resolved prior to this standard being ready for vote.</p> <p>The most significant issues include clarification on what is in scope and out of scope for the standard. Clear definitions will help in this effort. In addition, listing what is out of scope for the standard (similar to what was done in the Urgent Action Standard 1200) would be helpful. For example based on the NERC webcast, it is our understanding that communication systems are out of scope (as well as nuclear).</p> <p>Inconsistencies between sections in the draft and other NERC or industry standards need to be addressed as well. It is our understanding that this standard will be reliant on or impacted by other NERC standards or policies that either exist, are being revised, or are under development (e.g. Standard 200, a telecommunication standard, a risk assessment guide or standard). It would be helpful to reference these standards within Standard 1300 when there is an overlap or touch point.</p> <p>Security efforts and requirements for EMS/SCADA systems, substation equipment/systems, and generator control systems can and should not always be the same (e.g. Section 1306 applies mainly to EMS/SCADA systems). These differences are further complicated if these systems are networked and utilizing routable protocol. Having separate sections/requirements in the standard for EMS/SCADA systems, substation equipment/systems, and generator control systems would help clarify these differences and the security expectations (e.g. splitting Section 1306 into 3 sub-sections).</p> <p>We believe that the incident reporting requirements</p>	<p>Definitions will be reviewed and the scope clarified in light of comments received.</p> <p>References to related NERC standards will be made to the extent possible.</p> <p>The drafting team will consider changes to section 1306 for clarity.</p> <p>The section on Incident Reporting will be clarified.</p> <p>The FAQ will be reviewed for accuracy.</p> <p>A draft implementation plan will be included with draft version 2 of this standard.</p> <p>FAQs cannot be included as part of the standard. The draft standard will be reviewed to clarify intent and minimize the need for FAQs.</p> <p>Timeframes will be reviewed for consistency.</p> <p>A compliance matrix will be available when the final version of the standard is posted for balloting.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>should only focus on security incidents. Equipment and system failures are common (e.g. modem problems or telephone equipment problems). These general incidents may not only be burdensome but may mask actual security incidents because of their volume.</p> <p>In the FAQs (Section 1304, question 3) different solutions are listed as a means of providing an electronic security perimeter. This is very helpful and could be expanded. Please note that one method listed does not necessarily meet the requirements of Section 1304.a.3 and has a known security weakness (i.e. dial-back modems do not usually provide logging capabilities and have proven to be an insecure means of user authentication because of dial-back spoofing).</p> <p>There is no implementation plan included in this draft. We appreciate that the drafting team on page 3 of this Comment Form acknowledges this and states that an implementation plan will need to take into account the time needed to attain compliance. Page 3 also states that a plan will be developed at a later date for posting with a subsequent draft of this standard. An implementation plan will be needed at the same time of a revised standard in order to determine if the standard is ready to go to ballot.</p> <p>General: Should or will the FAQs be part of standard? The FAQ provided a great deal of clarification of the intent of the standard. It is preferred that the standard be reworked to avoid the need for a separate document to assist in its interpretation. At the very least, the FAQ's need to be made consistent with Standard 1300 and referenced by the standard.</p> <p>General: The standard does not specifically address whether protective relays connected via non-routable protocols are in scope or not. The original urgent action item 1200 specifically excluded electronic relays installed in generating stations, switching stations, and substations. The only reference to protection systems is special protection systems in the new standard.</p>	

Name	Company	Response	Comment	Drafting Team Response
			<p>Standard relaying systems (used to isolate faulted elements) are not specifically included or excluded from the new NERC 1300 standard.</p> <p>An inconsistent timeframe for removal of access after an employee's change in status is used in the standard. In section 1301.a.5.iv, access to a critical cyber access should be accomplished within 24 hours of a change in user access status. Again in section 1303.1.4.iii (1303.b.4.iii), a 24 hour timeframe is mentioned. Section 1306.b.2 says Upon normal movement of personnel out of the organization, management must review access permissions within 5 working days. A 5 day timeframe for normal movement (transfers, etc) is more reasonable. Clarification should be provided.</p> <p>At the end of each of the eight sections of the standard it states, Sanctions shall be applied consistent with the NERC compliance and enforcement matrix. Will the matrix be included in the standard or should there be a specific reference where this is located/maintained (e.g. separate document or standard)?</p>	



Name	Company	Response	Comment	Drafting Team Response
Robert E. Strauss	New York State Electric and Gas Corp.	No	<p>1. In general, there are too many areas which require interpretations which are defined or included in the FAQ's. Since the FAQ's would not be part of the approval these interpretations need to somehow be included within the standard.</p> <p>2. An alternative to developing a definition of Bulk Electric System would be to require the Reliability Authority for each Control Area to identify the Bulk Electric System for its respective Control Area. The next step would be for each Responsible Entity to identify the Bulk Electric System Asset they are responsible for in that system, identify the critical operating system functions and tasks and then identify the Critical Cyber Assets.</p> <p>3. This standard is not consistent in the level of detail for each area being addressed. Also there is no process indicated for change to be made following approval. A different approach to consider would be to make the standard identifying roles and responsibilities; identification of what is required to be included within the standard and its objective; and the process for review and sanctions. A description of minimum level for each area or standard should be attached as a guideline. In that manner the Standards can be permanent and only adjust the attachment if warranted. The way the standards read now, they must be adhered to unless the responsible individual in the company grants an exemption or deviation. A standard should be a standard with no deviation. Minimum guidelines would be a more practical approach. A deviation or exemption to a guideline is a more pragmatic approach.</p> <p>NYSEG also concurs with the following NPCC comments:</p> <p>NPCC's participating members recommend that the</p>	<p>The standard will be reviewed to clarify intent and to minimize interpretation.</p> <p>Definitions will be reviewed in light of comments received.</p> <p>The draft standard will be reviewed for consistency and clarity. A change process is described in NERC's Standards Process Manual.</p> <p>The definitions have been modified.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>definition of Critical Cyber Assets be;</p> <p>"Those cyber assets that enable the critical bulk electric system operating tasks such as monitoring and control, load and frequency control, emergency actions, contingency analysis, arming of special protection systems, power plant control, substation control, and real-time information exchange. The loss or compromise of these cyber assets would adversely impact the reliable operation of bulk electric system assets. (We have recommended this verbiage be used in 1302).</p> <p>NPCC's participating members do not agree with definition in 1302.a.1. and recommend that NERC create a Glossary of Definitions that the NERC Standards can reference and that this Glossary pass through the NERC SAR-Standard process.</p> <p>NPCC's participating members recommend changing the Incident definition from</p> <p>"Incident: Any physical or cyber event that: disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset, or compromises, or was an attempt to compromise, the electronic or physical security perimeters."</p> <p>to</p> <p>"Incident: Any physical or cyber event that: disrupts, or could have lead to a disruption of the functional operation of a critical cyber asset."</p>	

Name	Company	Response	Comment	Drafting Team Response
Robert Pellegrini	United Illuminating	No	<p>Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue. NPCC's participating members also believe the need to change the Incident definition, to the one shown in Question 1 is important.</p> <p>As previously discussed and commented on in various forums, NPCC supports the NERC decision to move away from monetary sanctions.</p> <p>NPCC's participating members have also expressed concern over the incremental administrative tasks and documentation requirements to be compliant with this standard and hopes the Standard Drafting Team will consider this during the development of the associated "Implementation Plan".</p> <p>Throughout the document, the compliance levels should be updated to measure the proposed revisions suggested below. NPCC has made some recommendations in this regard.</p> <p>There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected and recognized with consideration of this Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to gauge the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is NPCC's hope that this will be considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.</p>	<p>The definitions will be reviewed in light of comments received.</p> <p>A draft implementation plan will be posted with the draft version 2 of this standard.</p> <p>The standard will be reviewed for consistency.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p>

Name	Company	Response	Comment	Drafting Team Response
Robert V. Snow P.E.	Robert Snow	No	<p>This document is much better than the prior document. It could use to include some actual testing of the systems proposed. Suggest adding:</p> <ol style="list-style-type: none"> <li>1. The requirement for an Intrusion Assessment by an independent agency once every three years with the requirement that any vulnerabilities be remedied within three months.</li> <li>2. Adopting a "defence in depth" approach rather than what reads like one barrier around the system and nothing after an entity gets past the first barrier.</li> <li>3. A network for information sharing about events and lessons learned between the cyber entities.</li> </ol> <p>In the Roles and Responsibilities:</p> <p>Senior Management of the respective entity must be responsible for providing sufficient resources (people and funding) to achieve the identified program and to provide additional resources to remedy any incidents or vulnerabilities that are identified.</p> <p>These standards should apply to all control rooms that have a role in performing the functions in 1302 (a) (1) (i). They would include backup facilities and secondary control rooms.</p>	<p>The requirements do not preclude a third-party assessment; however, the drafting team does believe this approach should be required.</p> <p>The drafting team believes the requirements of this standard do constitute a defense in depth approach.</p> <p>The industry employs the IAW SOP to report incidents to the ES ISAC.</p> <p>The drafting team cannot dictate staffing or funding requirements.</p> <p>Backup facilities are not specifically excluded; however, their inclusion will be based on applicable entities' risk assessments.</p>

Name	Company	Response	Comment	Drafting Team Response
Roman Carter	Southern Company	No	<p>General Comments</p> <p>As the standard expands in its scope from the centralized EMS systems to include any cyber asset deemed critical to serving customers, it is also vastly expanding in scope to the types of devices it must cover. It appears to still be focused on Unix/Windows 'IT Shop' type assets exclusively. Much care needs to be taken in future drafts that requirements are not made on 'cyber assets' that can't be met by devices in the field. One specific example is the standard requires that all cyber assets SHALL present an appropriate use banner.</p> <p>In numerous places the standard states that 'the document or set of documents shall verify that all critical cyber assets are within the security perimeters'. It is unclear how any document can verify this. Some non-compliance measures are even based on whether the document verifies this. Please clarify how a document verifies completeness.</p> <p>In several measures, especially those dealing with perimeters, there is no recognition of scale. The standard and FAQ call for in some instances single computers, single RTU's, and single modems to have their own perimeter therefore there could literally be several hundred if not thousands of perimeters. This will only grow as an issue over time as more devices become IP capable. A problem with any single perimeter, no matter how insignificant or even whether it was security related makes you at most 88% compliant with the standard (missing 1 out of 8) for the year. This is a large disincentive and the all-or-nothing nature of these measures distorts reality from a compliance reporting perspective.</p> <p>All measures based on 'gaps in logs' need to move to some more meaningful measure. The problems with this 'gap' approach are many. It doesn't scale to the potentially hundreds or thousands of perimeters that may be required, it doesn't recognize the risk of any</p>	<p>A "technology permitting" clause will be added.</p> <p>The language will be modified to clarify that it is the applicable entities who are required to document that all critical cyber assets are within the security perimeters and must be able to produce that documentation for compliance monitoring purposes.</p> <p>The drafting team believes that narrowing the perimeters will make implementation easier rather than more difficult.</p> <p>The drafting team will reconsider the level of non-compliance.</p> <p>The compliance monitoring section is a required element of all NERC standards.</p> <p>Section 1303 addresses third-party and business partner issues. The standard will be reviewed to add clarity to this point.</p> <p>The standard requires that critical cyber assets inside the substation must be protected, not the entire substation.</p> <p>Timeframes will be reviewed for consistency.</p> <p>The standard will be reviewed for consistency.</p> <p>The exclusion of nuclear units will be added to the applicability section.</p> <p>Definitions will be reviewed in light of comments received.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>particular gap, there are no lower bounds on the gaps (switching a tape in a video monitoring system makes you non-compliant, as does rebooting your cardkey systems), large gaps in access logs can be caused by such things as hurricanes or mandatory evacuations or fiber cuts, which should not make one non-compliant with a cyber security standard.</p> <p>Numerous times in the standard details of the compliance monitoring process are included. It seems that since compliance is a regional matter that these details are better left to the regional compliance enforcement plans. See (1303)(n)(1) as an example.</p> <p>The standard as written seems to imply that the critical cyber asset is under the direct control of the applicable entities mentioned (i.e. located within physical perimeter managed by the entity). In many cases the cyber asset may be used by the entity on its site but is actually managed and/or located remotely by an application service vendor. This is the case for tagging services by much of the industry and is used by NERC itself for the Interchange Distribution Calculator and System Data eXchange. To what extent will the entity subscribing to an application service be held accountable under compliance for the activities (e.g. many of the requirements of 1306) of the vendor providing the services? In many, if not most, cases the entity will have no control over the procedures used by a third party application service provider in the areas covered by 1306.</p> <p>The physical protection of substations is a good concept but impractical. Thousands of dollars would be spent at each facility to monitor access to a facility that has an eight-foot cyclone fence around equipment that is often remotely controlled from receivers on top of poles. An incident on the transmission lines, outside the substation, would have basically the same effect as an incident inside the substation. Damage to these unmanned substations could be as easily inflicted from outside the cyclone fence as from inside.</p>	

Name	Company	Response	Comment	Drafting Team Response
------	---------	----------	---------	------------------------

Cross references throughout the standard need to be corrected.

For all requirements and measures - all time periods for changes in status of user access should be changed across the board to five (5) working days for normal movement and 24 hours for involuntary terminations. The time period to change should begin as soon as access is no longer required to account for transition periods.

The existence of consistency issues on all levels for all requirements needs to be investigated.

The standard needs to explicitly exclude nuclear facilities as stated in the Final SAR.

Please clarify which generation facilities are subject to the standard.

According to the FAQ on section 1302, Question 2, the bulk electric system is 35kV or higher. The definition of 'Bulk Electric System' according to the NERC By-Laws is "A bulk electric system is defined as that portion of an electric utility system, which encompasses the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Please clarify this difference.

Name	Company	Response	Comment	Drafting Team Response
S. Kennedy Fell	New York Independent System Operator	No	<p>As previously discussed, the NYISO supports NERC decision to move away from monetary sanctions, however the NYISO would like to reinforce their position the it does not support monetary sanctions.</p> <p>The NYISO is concerned about the incremental administrative tasks and documentation requirements to support the 1300 standard. With the increased requirements within the 1300 standard , the NYISO believes the requirements need to be phased in over 1 to 2 years. Additionally, audit compliance would commence after the entity is to be fully compliant.</p> <p>Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1.</p> <p>The references within the standard made to other portions of Standard 1300 are not correct. For example, 1301.a.3 says "as identified and classified in section 1.2." Each one of these incorrect references must be corrected.</p> <p>Throughout the document, the compliance levels need to be updated to measure the proposed revisions suggested below.</p> <p>Confidentiality and disclosure is a growing concern as the industry moves towards mandatory standards. There should be a statement in the Standard to address confidentiality to say that all applicable confidentiality agreements and documents will be respected with consideration of this and all Standard.</p> <p>The standard, as drafted, has a number of new requirements that presently do not exist in the Urgent Action Standard #1200. In order to guage the impact of these new requirements and make viable plans to achieve compliance, it is essential to understand how the standard will be implemented and the associated timeframes or schedules for the various subsections of the Standard. It is the NYISO's hope that this will be</p>	<p>A draft implementation will be posted with draft version 2 of the standard. A phased approach will be used.</p> <p>The standard will be reformatted and references corrected.</p> <p>The standard will be reviewed for consistency.</p> <p>The issue of audit data confidentiality will be brought to the Vice President -- Compliance at NERC.</p> <p>A draft implementation will be posted with draft version 2 of the standard.</p>



Name	Company	Response	Comment	Drafting Team Response
			considered during the Drafting Team's development of the Implementation Plan scheduled to be drafted and posted with the next posting of this Standard.	
Seiki Harada	BC Hydro	No	I suggest we deal with the points raised in Question 3 next, before putting it to ballot.	See section by section comments.
Shelly Bell	San Diego Gas and Electric	No		
Stacy Bresler	PacifiCorp	No	Clarity in definations. The details are crititcal to proper implementation and auditing.	The definitions will be reviewed in light of comments received.

Name	Company	Response	Comment	Drafting Team Response
Terry Doern	Bonneville Power Administration	No	<p>The first page of the standard must include a statement of scope developed by NERC CIPC. The scope must be absolutely clear as to the standard's purpose and to what it applies. The definitions of terms should follow. The definitions should define terminology used within the standard, but not be used to define the scope of the standard. A standard must be prescriptive in it's use of terms in order to establish a uniform baseline for compliance.</p> <p>1. BPA and other utilities may have conflicts between NERC 1300 and applicable cyber security related laws, guidelines, policies and regulations (e.g., U.S. Federal, State, Canadian, etc.). A process to resolve these conflicts will need to be developed by NERC and the affected utilities.</p> <p>2. Technical issues at the systems level may limit the ability to follow this standard. Exceptions may be needed, therefore a process to resolve these issues will need to be developed by NERC and the affected utilities.</p> <p>3. This Standard contains policy statements and should be acknowledged as such in order to be in alignment with the CYBER SECURITY industry.</p> <p>4. Consider removing selected timeframe references (e.g., quarterly, annually, etc.) and replace with "to ensure compliance with the entities documented processes." This would ensure that the entity documents their processes and procedures, while providing them the flexibility to define their own auditable/measurable business rules.</p> <p>8. In all sections, compliance monitoring doesn't appear to synchronize with the section introduction paragraph, requirements, and measurements sections.</p> <p>9. The compliance section is very difficult to understand. Multiple compliance levels are complex</p>	<p>The purpose statement will be redrafted. Definitions will be reviewed in light of comments received.</p> <p>Authorized exceptions are acceptable as described in 1301. A "technology permitting" clause will be considered.</p> <p>The standard contains requirements. Applicable entities' security policies address these requirements.</p> <p>The drafting team believes that the diversity of entities and their business processes defines the need for minimum acceptable timeframes.</p> <p>The standard will be reviewed for consistency.</p> <p>NERC's compliance program has established the four-tiered non-compliance model.</p> <p>A compliance matrix will be available when the standard is posted for balloting. A draft implementation plan will be posted with draft version 2.0 of this standard.</p>

Name	Company	Response	Comment	Drafting Team Response
			and should just be that you are compliant or non-compliant.	
			10. It is difficult to comment on the compliance section without understanding how the sanctions and fines are going to be imposed.	
Tom Flowers	CenterPoint Energy	No		

Name	Company	Response	Comment	Drafting Team Response
Tom Pruitt	Duke Power Company	No	<p>Given the critical role played in today's environment, why is the PSE excluded from meeting this standard? The LSE IS included, though the FAQ indicate that loss of load, in and of itself, is not a NERC reliability concern. This is, at best, inconsistent application of this standard. Given the critical role of the PSE in today's environment, the PSE should be included.</p> <p>Explicitly state that nuclear facilities are excluded from this standard as is stated in the SAR.</p> <p>Since the Drafting Team has structured the standard so that individual entities are charged with defining the scope of assets subject to this standard, this limitation needs to be spelled out. The draft states that risk assessment of bulk electric assets and all cyber support assets is part of the standard. The standard should also identify another risk assessment of cyber assets to determine their scope. More clarity is needed on the number and types of assessments. How many steps are there 1, 2, or 3? How is this communicated across ISO and other third party arrangements for conducting operations on the grid?</p> <p>Administrative Costs Overall the required processes and frequency of execution are a major concern and likely cost prohibitive to implementation at Duke Energy Corporation. While Duke Energy agrees with the intent and general nature of the proposed 1300 standard, many of the specific requirements imply significant administrative costs to develop and maintain a significant number of new processes. (A simple change would be to reduce implementation costs by reducing the frequency of executing the processes.) This is a common concern across a number of operational units at Duke Energy. One example is the definition of "incident" and the further inclusion of this term in several requirements that would mean the</p>	<p>NERC's mission does not extend to the PSE.</p> <p>The exclusion of nuclear units will be added to the applicability section.</p> <p>The standard states explicitly that entities are to use their own risk assessment methodology to define their critical cyber assets.</p> <p>The term security incident will be redefined and the reporting of security incidents modified to reflect the change in definition.</p> <p>The drafting team does not believe that the standard prohibits such an approach.</p> <p>The amount of documentation required for this standard reflects its wider scope and depth of detail.</p> <p>It is up to the entity to ensure that third parties whose personnel have access to critical cyber assets have certified that their personnel have been screened.</p> <p>A "technology permitting" clause will be considered.</p> <p>The standard will be reviewed for consistency.</p> <p>Timetable references will be reviewed for consistency.</p> <p>A draft implementation plan will be posted with draft version 2 of this standard.</p>

Name	Company	Response	Comment	Drafting Team Response
			<p>logging and reporting of thousands of discrete events per day. Limiting incident processing to the term defined as "security incident" significantly reduces the administrative burden, but continues to focus on the cyber security health of the bulk power systems that should be monitored.</p> <p>As well, a large burden is placed on executive senior management to review and approve what could be large number of NERC 1300 related items. This manager should be allowed to delegate this administrative overhead, but maintain the overall responsibility of providing governance to the NERC 1300 regulated company entities.</p> <p>A majority of the burden is through record keeping and reporting – which have their place, but are dominant in this standard. The cost benefit for such administrative burden is simply not apparent.</p> <p>Personnel Related Concerns</p> <p>Another high-level concern is the cost of implementing the personnel-oriented processes described in this draft of 1300. Like many other energy companies, much of the work force at Duke has become contracted or third-party based. Background checks, training, and other regulations that are not particularly burdensome when addressed over time with full-time employees, become quite problematic with transient, contracted, part-time labor forces, affecting direct and administrative costs.</p> <p>Costs</p> <p>Many of the technical requirements of the proposed 1300 standard are either not technically possible with legacy systems or very expensive to implement. Examples include such things as strong passwords, system logging, and procuring and developing complete test systems. This includes physical security implementation (fossil control rooms), site access (cameras at sub-stations) and building physical rooms to isolate equipment.</p>	

Name	Company	Response	Comment	Drafting Team Response
			<p>Narratives /Requirements/Measures/FAQs are Inconsistent</p> <p>Measures don't match the actual requirements. For example, background checks are more strictly defined in the measures than they are in the requirements.</p> <p>Answers provided in the FAQ's in some cases do not match wording in the standard. In other places, narratives, measures, and requirements do not match. Wording should be consistent throughout each section.</p> <p>There should also be some consistency in the timeframes required to remove user-ids and permissions. It is confusing trying to remember what is 24 hours, 48 hours, etc. Compliance planning will need adequate time to put into place.</p> <p>What is the anticipated timeline for implementation? It would take an extended period of time to get initial 5 year background checks completed for larger entities. Will the plan be phased in over time?</p>	

Name	Company	Response	Comment	Drafting Team Response
Tony Eddleman	Nebraska Public Power District	No	<p>A major issue is the new requirement to classify information and will significantly drive up costs to customers as currently written. This will require additional resources (labor, background checks, etc.) to implement. Our business is to generate and transmit energy. This new requirement could require a classification on a large portion of the documents that we use daily. This will affect a significant number (virtually all) of the employees in a utility, vendors, individuals in public office, such as our Power Review Board, etc. Then, for a person to have access to that information will require a background check that is renewed every five years. This standard requires significant "paperwork" and "red tape". How do you mark electronic files? More specifics are needed on how to classify information and a cost / benefit analysis should be performed on this requirement. I support cyber security for critical assets and feel this is an important standard to implement. As currently written, this standard will be very resource intensive to implement.</p>	<p>Classification levels are used to minimize access to information about critical cyber assets. Without such controls, the ability to protect those assets is at risk.</p>

Name	Company	Response	Comment	Drafting Team Response
Victor Limongelli	Guidance Software, Inc.	No	<p>In addition to the general statements regarding the need for incident response planning in 1307 (which focus only on "Incident Classification," unspecified "Response Actions," and Reporting), the Standard should detail the technical and procedural requirements for an effective cyber security incident response plan. As written, the Standard would allow each organization to define for itself the appropriate level of incident response actions and incident handling procedures. Unfortunately, this approach lowers the overall grid's reliability. The investigation of, and response to, a cyber security incident involving one or more entities or grids can run aground at the vulnerable organization that does not have an effective incident response capability. Thus, the failure of certain organizations can impact other entities, as well as the overall grid. In short, including within the Standard a baseline level of acceptable incident response capabilities will help ensure the integrity and reliability of the interconnected electric systems of North America.</p> <p>Fortunately, the Standard need not attempt to develop the appropriate minimum standards. Earlier this year, the National Institute of Standards and Technology ("NIST"), pursuant to authority established by the Federal Information Security Management Act of 2002 ("FISMA"), issued Special Publication 800-61, entitled "Computer Security Incident Handling Guide" (the "NIST Guide," available at <a href="http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf">http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf</a>). The NIST Guide sets forth detailed technical, procedural, and policy guidelines for the implementation of a comprehensive incident response capability, consisting of four broad categories: (1) Preparation, (2) Detection and Analysis, (3) Containment, Eradication, and Recovery, and (4) Post-Incident Activity.</p> <p>By way of example, within the category of Containment, Eradication, and Recovery, the NIST</p>	<p>The drafting team believes that the flexibility to define individual response plans is more acceptable to a majority of the industry. However, NIST guidance will be referenced in the FAQs.</p>



Name	Company	Response	Comment	Drafting Team Response
			<p>Guide calls for the following key technical processes and methodologies for effective incident response:</p> <ol style="list-style-type: none"> <li>1. Immediate response capability. NIST comments: "It is generally desirable to acquire evidence from a system of interest as soon as one suspects that an incident may have occurred."</li> <li>2. Initial System Snapshot. In addressing this critical aspect of incident response, NIST correctly notes that: "Many incidents cause a dynamic chain of events to occur; an initial system snapshot may do more good in identifying the problem and its source than most other actions that can be taken at this stage."</li> <li>3. Analyze live systems with minimal invasiveness. The NIST Guide notes that without proper procedures, "risks are associated with acquiring information from the live system. Any action performed on the host will alter the state of the machine..."</li> <li>4. Volatile data acquisition and analysis: The NIST Guide provides: "...it is often desirable to capture volatile information that may not be recorded in a file system or image backup, such as current network connections, processes, login sessions, open files, network interface configurations, and the contents of memory. This data may hold clues as to the attacker's identity or the attack methods that were used."</li> <li>5. Forensic hard drive data acquisition. The NIST Guide provides clear direction on this issue: "After acquiring volatile data, an incident handler with computer forensics training should immediately make a full disk image ... (which) preserves all data on the disk, including deleted files and file fragments."</li> <li>6. Computer forensic analysis. Section 3.3.2 of the NIST Guide states: "Computer forensics software is valuable not only for acquiring disk images, but also for automating much of the analysis process, such as: <ul style="list-style-type: none"> <li>• Identifying and recovering file fragments and</li> </ul> </li> </ol>	

Name	Company	Response	Comment	Drafting Team Response
			<p>hidden and deleted files and directories from any location (e.g., used space, free space, slack space)</p> <ul style="list-style-type: none"> <li>Examining file structures, headers, and other characteristics to determine what type of data each file contains, instead of relying on file extensions (e.g., .doc, .jpg, .mp3)</li> <li>Displaying the contents of all graphics files</li> <li>Performing complex searches</li> <li>Graphically displaying the acquired drive's directory structure</li> <li>Generating reports."</li> </ul> <p>7. Establish a Proper Chain of Custody with a Message Digest Hash Algorithm.</p> <p>8. Log file acquisition and analysis.</p> <p>9. Ability to correlate multiple time zones of acquired media.</p> <p>10. Validated computer forensics technology via courts and independent testing, as stated by NIST: "Evidence should be collected according to procedures that meet all applicable laws and regulations . . . so that it should be admissible in court."</p> <p>These and the other detailed requirements set forth in the NIST Guide should be applied to entities performing the Reliability Authority, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, and Load Serving Entity. The Standard can accomplish this by incorporating the NIST Guide by reference. In addition to the benefit of establishing a baseline for each entity's incident response capability, incorporating the NIST Guide has the following advantages: (1) increasing the coordination between entities in the event of a cyber security incident, since each entity's incident response plan will include similar technical processes and procedural steps; (2) providing evidence</p>	

Name	Company	Response	Comment	Drafting Team Response
			of due diligence in the event that there is ever a federal investigation of a cyber security failure within the bulk electric system, and (3) standardizing the industry on an approach already required of certain entities (federal utilities).	
William J. Smith	Allegheny Energy	No	<p>The most significant concern is that this standard does not appropriately address the diverse environments of centralized power control centers, power stations and transmission substations. Implied in the standard is an environment similar to that of a central power control center. The physical, computing, and user environments are very different in each of these types of facilities. Revise the standard to accommodate the environments for each of these.</p> <p>Specific to power stations and substations, a separate physical perimeter for critical cyber assets may be difficult to reliably and completely achieve in all cases, while at the same time not providing additional benefit. Control rooms are a good example of this because a power station provides much easier sabotage targets once an individual is inside the plant. Revising the standard to require only a protected electronic perimeter and a physically protected perimeter where appropriate and beneficial for these diverse environments is appropriate.</p> <p>Revise the standard to separate logical user access requirements into 2 categories: 1) accessing assets from outside the protected electronic perimeter, and 2) accessing assets from inside the protected electronic perimeter. Revise the standard to make provisions for user access points (operator console) inside the electronic perimeter that must always be available for use and cannot be password protected.</p>	<p>The standard was drafted to address a diversity of environments.</p> <p>Critical cyber assets must be protected from threats outside and insider threats. Creating security perimeters to control access to these assets helps achieve this goal.</p> <p>The drafting team believes that standard supports this distinction.</p>

# Section 1301 Comments and Drafting Team Responses

Name	Company	Comments	Drafting Team Response
A. Ralph Rufrano	NYPA	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional</p>

Name	Company	Comments	Drafting Team Response
		to	differences, then we would include the differences under the "Regional Differences" section.
		"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.	1301.5.2.3 Changed wording to "An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits	

Name	Company	Comments	Drafting Team Response
		<p>on RS 1300, carried out by the compliance monitor</p> <p>1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Allen Berman	LIPA	<p>1301 Security Management Controls:</p> <p>(a)Requirements</p> <p>(2) Information Protection</p> <p>(ii) Classification</p> <p>Comment: Suggest changing paragraph to say "The responsible entity shall classify information related to critical cyber assets to aid personnel with access to this information in determining which and how information can be disclosed without jeopardizing its physical or cyber security. The relative sensitivity of information that should not be disclosed outside of the entity without proper authorization should be identified as well.</p> <p>(a)Requirements</p> <p>(3) Roles and Responsibilities</p> <p>Comment: Where is Section 1.2 that is referenced in the following sentence? "Roles and responsibilities shall also be defined for the access, use, and handling of critical information as identified in section 1.2."</p> <p>(a) Requirements</p> <p>(5) Access Authorization</p> <p>(iv) Access Revocation / Changes</p> <p>Comment: Suggest that modifications, suspensions, and terminations of user access be authorized, implemented, and documented in 24 hours only if a user is terminated for disciplinary action. In other cases, suggest that up to 5 business days be permitted. This requirement should also be listed as a measure in section (b).</p> <p>(b) Measures</p> <p>(3) Roles and Responsibilities</p> <p>(ii)</p> <p>Comment: Suggest changing "... shall be identified by name, title, phone, address, and date of designation" to "...shall be identified by name, title, business phone, business address, and date of designation."</p> <p>(b) Measures</p> <p>(5) Access Authorization</p> <p>(iii)</p> <p>Comment: Suggest changing "... shall identify each designated person by name, title, phone, address, and date of designation" to "...shall be identified by name, title, business phone, business address, and date of designation."</p> <p>(b) Measures</p>	<p>1301.a.2.ii - Section re-worded</p> <p>Section 1.2 changed to read 1301.1.2</p> <p>1301.1.5.4 Access Revocation section re-worded to permit the entities to define the processes that work best for their environments and protect their critical cyber assets.</p> <p>Phone and address changed to business phone and business address.</p> <p>Measures)</p> <p>Authorization to Place Into Production)</p> <p>Wording changed to "...shall have a defined process that maintains a current list..." How an entity updates and maintains the list of designated personnel is up to each entity. The word "current" implies that the entity will update their list in a timeframe that allows an audit process to verify that the list is not out of date.</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>(d) Compliance Monitoring Process - Changed the word "Audit" to "Documented Review". This allows each entity to determine how Compliance monitoring will be done.</p> <p>Changed "The list of designated personnel responsible to authorize access to critical cyber assets" to "The list of approving authorities for critical cyber information assets."</p>

Name	Company	Comments	Drafting Team Response
		<p>(6) Authorization to Place Into production  Comment: Suggest modifying "... shall be documented within 48 hours of the effective change" to "... shall be documented within 2 business days of the effective change".</p> <p>(d) Compliance Monitoring Process  (3)  (iv)  Comment: This section states that audit results for the information security protection program should be made available to the compliance monitor upon request. The standard requires periodic reviews of security access and various policies and procedures but does not state that formal audits be performed. Please clearly state this requirement and detail what audits should be performed.</p> <p>(d) Compliance Monitoring Process  (3)  (v)  Comment: Suggest changing "The list of approving authorities for critical cyber information assets." to "The list of individuals authorized to disclose information related to critical cyber assets."</p>	



Name	Company	Comments	Drafting Team Response
Bill Wagner	Calpine	<p>Page 3, Section 1301 Security Management Controls, (a) Requirements, (2) Information Protection, (i) Identification: Add requirement/clarification for meaningfully identifying information. For example, if a row in a database table records information about a critical cyber asset, must that row be identified in any specific way, or is it sufficient to simply say that information is documented in the asset inventory database?</p> <p>Page 3, Section 1301 Security Management Controls, subsection (3) Roles and Responsibilities, I recommend using critical cyber asset administrator rather than custodian to refer to someone that is responsible for day-to-day operation of the cyber asset (i.e., making sure the computer stays up and running, has adequate disc space, backups are made, etc.).</p> <p>Page 4, Section 1301 Security Management Controls, (a) Requirements (5) Access Authorization (iv) Access Revocation/Changes - in some cases 24 hours to revoke access may be unacceptable, in which case additional security and/or surveillance may be required until normal access is resecured.</p> <p>Page 5, Section 1301 Security Management (b) Measures (5) Access Authorization (iii) - remove or clarify (which) address of designated person.</p>	<p>1301.a.2.i - The standard simply states that you must identify your critical cyber asset information. If that information is contained in a database, then the entire database would be identified as containing critical cyber asset information and protected accordingly.</p> <p>1301.3 - Drafting team disagrees - The terms owner, custodian, and user are generic terms to identify the 3 basic roles personnel when it comes to the handling of information. How you identify these roles is up to you.</p> <p>1301.a.5.iv - This section has been re-worded</p> <p>1301.b.5.iii - Changed "address" and "phone" to read "work address" and "work phone".</p>

Name	Company	Comments	Drafting Team Response
Charles Yeung	SPP	<p>1301 (b) (1) (iv) Cyber Security Policy: Does the requirement to document extensions to deviations or exemptions presume that deviations and exemptions have an automatic expiration date coincident with the annual review? If not, why would extensions even be necessary?</p> <p>1301 (b) (5) (i) Does Access Authorization refer to 5 calendar days or 5 business days?</p> <p>1301 (b) (6) Does the reference to 48 hours refer to 2 calendar days or 2 business days?</p>	<p>1301.b.1.iv - An example of an exemption would be something like not being able to comply because of limitations of legacy hardware. This exemption would be in effect until such time as the hardware will support the standard. All exemptions and deviations should be time-bound. Any deviation or exemption that exceeds 12 months would need to be reviewed on an annual basis.</p> <p>1301.b.5.i - Section has been re-worded</p> <p>1301.b.6 - Section has been re-worded</p>

Name	Company	Comments	Drafting Team Response
Charlie Salamone	NSTAR	<p>1301.a.5.iii - Need to identify frequency of access reviews.</p> <p>1301.a.6 - Should be 24 business hours (1 business day) v. 24 hours. This is referenced throughout the document. Make this consistent throughout the document.</p> <p>1301.b.6 - Should be 48 business hours (2 business days) v. 48 hours. This is referenced throughout the document. Make this consistent throughout the document.</p>	<p>1301.a.5.iii - See Measures section</p> <p>1301.a.6 - Section has been re-worded</p> <p>1301.b.6 - Section has been re-worded</p>

Name	Company	Comments	Drafting Team Response
Charlie Salamone	NSTAR	<p>1301.a.5.iii - Need to identify frequency of access reviews.</p> <p>1301.a.6 - Should be 24 business hours (1 business day) v. 24 hours. This is referenced throughout the document. Make this consistent throughout the document.</p> <p>1301.b.6 - Should be 48 business hours (2 business days) v. 48 hours. This is referenced throughout the document. Make this consistent throughout the document.</p>	<p>1301.a.5.iii - Specified in the "Measures" section.</p> <p>1301.a.6 - Section re-worded</p> <p>1301.b.6 - Section re-worded</p>

Name	Company	Comments	Drafting Team Response
Chris DeGraffenried	NYPA	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Dave Magnuson	Puget Sound Energy	<p>1301 Security Management Controls (a) (2) (i) Clarify meaning of "floor plans" -- at what level of detail are we protecting. Should clarify only those floorplans with information pertaining to critical cyber assets. Example: Facility fire evacuation plans often show high level detail of floor plans.</p> <p>1301 Security Management Controls (a) (3) Clarify if there can be more than one senior management responsible for the standard</p> <p>1301 Security Management Controls (a) (5) (iv) 24-hour access change requirement should apply to termination for cause only; lengthen period for personnel transfers, etc.</p> <p>1301 Security Management Controls (d) (2) Clarify compliance monitor -- who serves this function.</p>	<p>1301.a.2.i - Section has been reworded for clarification.</p> <p>1301.a.3 - There should be only one senior management person responsible for the standard. This person can delegate responsibility but it is this person who leads and is accountable for the success of the program.</p> <p>1301.a.5.iv - Specific timeframes removed.</p> <p>1301.d.2 - Whoever you reported up to for the NERC 1200 would be the compliance monitor. NERC is the compliance monitor at the uppermost level. Each regional authority can monitor their own region and report to NERC.</p>



Name	Company	Comments	Drafting Team Response
Dave McCoy	Great Plains Energy	<p>1301 - Under Compliance Monitoring Process Item (3) (v) it states that audit results and mitigation strategies be made available to the compliance monitor upon request. Is this just the results of internal reviews that are required under these standards or is this suggesting that a full audit be performed annually on standard compliance? If so, is the expectation that 3rd parties perform such audits? It would be helpful to clarify what is meant by audits.</p> <p>1301 - Under Requirements under Information Protection under Identification it says, The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information. Question 2 under 1301 in the Frequently Asked Questions states that Some examples of critical information would be grid maps, network connectivity diagrams,... The 1300 list appears to be critical cyber asset related, while the FAQ list is bulk electric system related. Is 1300 intended to address the protection of bulk electric system information that is maintained completely separately from any critical cyber asset?</p> <p>1301, 1303, 1306 -- There are multiple references to the time frame for implementing access changes. (See list of references below.) It would be helpful if the requirements were stated clearly and centralized in one place:  1301 (a) Requirements (5) Access Authorization (iv) Modification, suspension, and termination of user access to critical cyber assets is accomplished with 24 hours of a change in user access status.</p> <p>1301 (e) Levels of Noncompliance (4) Level Four (xi) Access revocation/changes are not accomplished within 24 hours of any change in user access status.</p> <p>1301 (a) Requirements (5) Access Authorization (iv) Modification, suspension, and termination of user access to critical cyber assets is accomplished with 24 hours of a change in user access status.</p> <p>1301 (e) Levels of Noncompliance (4) Level Four (xi) Access revocation/changes are not accomplished within 24 hours of any change in user access status.</p>	<p>1301.d.v - Compliance Monitoring Process - Word "Audit" changed to "Documented review results". Entities will decide who will conduct this.</p> <p>1301.a.2.i - Section has been re-worded to be more specific. FAQ was provided as an aid only and will not be part of the final standard.</p> <p>1301.a.5.iv - References to timeframes surrounding access changes/revocation has been changed to better reflect business needs.</p> <p>1301.e.4.xi - Removed.</p>

Name	Company	Comments	Drafting Team Response
Dave Norton	Entergy Transmission	13. Page 3 - Requirements are prefaced with "At a minimum", but the defined requirements seem to be all inclusive. Critical cyber asset definitions are very broad and may lead to some unanticipated results and inclusiveness. In applying the definition of critical cyber asset, non-critical assets appear to become critical either based on their location within the electronic security perimeter or the presence of "out of band" dial-in modems/ports. Can this lead to a situation where more assets fall in- scope under the Standard as being "critical" than was intended?	Each entity will have to determine whether or not information is to be considered critical cyber asset information. A non-critical asset that is within the electronic security perimeter may not have critical cyber asset information on it and therefore, would not fall under the same requirements. Access to that asset must be controlled simply because its location in the network is within the electronic security perimeter and can provide access to the defined critical cyber assets.

Name	Company	Comments	Drafting Team Response
David Kiguel	Hydro One	<p>Change 1301.a.2 from</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets."</p> <p>Change 1301.a.2.i from</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centres, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well."</p> <p>Change 1301.a.5.iv from</p> <p>"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."</p> <p>to</p> <p>"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented."</p>	<p>1301.a.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.a.2.i Drafting team agrees. Wording changed.</p> <p>1301.a.5.iv Wording changed to eliminate specific timeframe.</p> <p>1301.d.3.iv Word "Audit" removed and replaced with "Documented review results".</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.a.3 Drafting team agrees. Wording changed.</p> <p>1301.b.5.i Specific timeframes removed.</p> <p>Days and Years have been changed to reflect either business or calendar timeframes.</p> <p>1301.d.3.ii - section re-worded.</p> <p>1301.d.2.iii - Changed wording to "An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist"</p> <p>1301.e.2.iii Changed wording to "An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist"</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>1301.5.4.11 removed</p>

Name	Company	Comments	Drafting Team Response
		<p>In 1301.d.3.iv, we request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor. No other audits are to be addressed by Standard 1300.</p> <p>We recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process and therefore each Region is responsible for designating the Compliance Monitor.</p> <p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>In Section 1301.a.3 change  "....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."</p> <p>The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.</p> <p>Change 1301.b.5.i from "5 days" to "7 calendar days".</p> <p>1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency.</p> <p>In 1301.d.3.ii, change "address and phone number" to "business contact information". Same on page 5, 1301.b.5.iii</p> <p>In 1301.e.1.iii, we request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>In 1301.e.2.iii, change from</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or"</p> <p>Remove 1301.e.4.v. The content is implied and redundant with 1301.e.4.i. If kept, change "Executive Management" to "Senior Management."</p> <p>In 1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for</p>	

Name	Company	Comments	Drafting Team Response
		cause or for disciplinary actions, or within 7 calendar days (FERC ORDER 2004b-Standards of Conduct).	

Name	Company	Comments	Drafting Team Response
David Little	Nova Scotia Power	<p>1301</p> <p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from; The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets. (some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.) to The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets.</p> <p>Change 1301.a.2.i from; The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information. to The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well. (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from; ....entity's implementation of... to ...entity's implementation and adherence of...</p> <p>The 24 hours in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.</p> <p>Change 1301.a.5.iv from; Responsible entities shall define procedures to ensure that modification,suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented. to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		<p>Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented. (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)</p> <p>change 1301.b.5.i from; 5 days</p> <p>to 7 calendar days (the 5 days may be not be sufficient time especially when considering holiday seasons)</p> <p>In 1301.d.3.iv, request clarification that this -audit - applies to only audits on RS 1300, carried out by the compliance monitor</p> <p>In 1301.d.3.ii, change from - address and phone number - to business contact information. Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals</p> <p>Recommend that under Regional Differences, it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>In 1301.e.1.iii, request clarification on -30 days of the deviation-. Also please explain the difference between -deviation and -exception. This does not match the FAQ 1301 Question 4.</p> <p>In 1301.e.2.iii, change from; An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or to An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change -Executive Management to -Senior Management- for consistency and clarity.</p> <p>In 1301.e.4.xi, repeat of the earlier 24 hours if a user is terminated for</p>	<p>been designated but a formal process to validate and promote systems to production does not exist"</p> <p>1301.5.4.11 removed</p>

Name	Company	Comments	Drafting Team Response
		cause or for disciplinary actions, or within 7 calendar days(should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).	



Name	Company	Comments	Drafting Team Response
David Little / Bonnie Dickso	Nova Scotia Power	<p>1301</p> <p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from; The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets. (some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.) to The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets.</p> <p>Change 1301.a.2.i from; The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information. to The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well. (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from; ....entity's implementation of... to ...entity's implementation and adherence of...</p> <p>The 24 hours in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.</p> <p>Change 1301.a.5.iv from; Responsible entities shall define procedures to ensure that modification,suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented. to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		<p>Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented. (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)</p> <p>change 1301.b.5.i from; 5 days</p> <p>to 7 calendar days (the 5 days may be not be sufficient time especially when considering holiday seasons)</p> <p>In 1301.d.3.iv, request clarification that this -audit - applies to only audits on RS 1300, carried out by the compliance monitor</p> <p>In 1301.d.3.ii, change from - address and phone number - to business contact information. Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals</p> <p>Recommend that under Regional Differences, it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>In 1301.e.1.iii, request clarification on -30 days of the deviation-. Also please explain the difference between -deviation and -exception. This does not match the FAQ 1301 Question 4.</p> <p>In 1301.e.2.iii, change from; An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or to An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change -Executive Management to -Senior Management- for consistency and clarity.</p> <p>In 1301.e.4.xi, repeat of the earlier 24 hours if a user is terminated for</p>	<p>been designated but a formal process to validate and promote systems to production does not exist"</p> <p>1301.5.4.11 removed</p>

Name	Company	Comments	Drafting Team Response
		cause or for disciplinary actions, or within 7 calendar days(should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).	

Name	Company	Comments	Drafting Team Response
Deborah Linke	U.S. Bureau of Reclamation	<p>1301 Security Management Controls</p> <p>Critical business and operational functions performed by cyber assets affecting the bulk electric system necessitate having security management controls. This section defines the minimum security management controls that the responsible entity must have in place to protect critical cyber assets.</p> <p>(a) Requirements</p> <p>(1) Cyber Security Policy</p> <p>The responsible entity shall create and maintain a cyber security policy that addresses the requirements of this standard and the governance of the cyber security policy. Suggest this be changed to read "... the governance of the cyber security controls." It is the controls that require governing, not the policy.</p> <p>(2) Information Protection</p> <p>The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets. Suggest this be changed to read "... cyber-based information pertaining to or used for critical business and / or operational functions. Protection controls shall address information in storage, in transit, and while being processed." Please reconsider the scope of information covered by this statement. Is it adequate?</p> <p>(ii) Classification</p> <p>The responsible entity shall classify information related to critical cyber assets to aid personnel with access to this information in determining what information can be disclosed to unauthenticated personnel, as well as the relative sensitivity of information that should not be disclosed outside of the entity without proper authorization. The authors may wish to consider using the term "categorize" in lieu of "classify" to ensure there is not confusion with "classified" information guidance and standards. Suggest this be "unauthorized" to address a broader audience. "Authenticated" personnel could be construed to only include those with proper log-in credentials.</p> <p>(5) Access Authorization</p> <p>The following should read:</p> <p>(i) The responsible entity shall institute and document a process for the management of access to information pertaining to or used by critical cyber assets where the compromise of such access could impact the reliability and/or availability of the bulk electric system for which the entity is responsible.</p>	<p>1301.a.1 Agreed. Wording changed</p> <p>1301.a.2 - Words "pertaining to or used by" changed to "associated with". The rest of section remains unchanged. Drafting team thinks that the section wording should not be too specific in order to allow entities to follow their own risk assessment procedures when identifying and classifying their critical cyber asset information.</p> <p>1301.a.2.ii - Word "classify" changed to "categorize". "Authenticated" changed to "authorized".</p> <p>1301.a.5 - Section re-worded.</p> <p>1301.a.5.i - No Change necessary</p> <p>1301.a.5.iii - See Measures section for review period.</p> <p>(6) Authorization to Place into Production has been moved under Governance and re-worded.</p>

Name	Company	Comments	Drafting Team Response
		<p>(ii) Authorizing Access</p> <p>The responsible entity shall maintain a list of all personnel who are responsible for authorizing access to critical cyber assets. Logical and physical access to critical cyber assets may only be authorized by the personnel responsible to authorize access to those assets. All access authorizations must be documented.</p> <p>(iii) Access Review</p> <p>Responsible entities shall review access rights to critical cyber assets to confirm they are correct and that they correspond with the entity's needs and the appropriate roles and responsibilities. How often? Unless this review is covered elsewhere, the authors may want to consider including the review period here. Certainly every 6 months is not out of the question. Sooner if practice.</p> <p>B(6) Authorization to Place Into Production</p> <p>Responsible entities shall identify the designated approving authority responsible for authorizing systems suitable for the production environment by name, title, phone, address, and date of designation. This information will be reviewed for accuracy at least annually. Changes to the designated approving authority shall be documented within 48 hours of the effective change. Is this time period practical? Suggest that a longer time be considered, perhaps one business week?</p>	

Name	Company	Comments	Drafting Team Response
Ed Goff	Progress Energy	<p>1301 Security Management Controls --</p> <p>a.2.ii Classification -- this requires a full data classification program. This needs to be defined. - a.5.iv Access Revocation/Changes -- given the new scope of critical assets included by the 1300 standard, the requirement to accomplish changes, authorize and document within 24 hours is not realistic. Notifications of employee changes may not be known company wide within 24 hours especially if change was a transfer or reassignment of duties where employee is not terminated from company. In final comment to the 1200 urgent action standard, NERC conceded that 24 hours may not practical and suggested an alternative stating: - that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence. In the case of contractor/vendor employees, they shall be required to promptly advise the system owner/operator when such changes occur and system access should be updated as soon as practical but no later than three business days after notification.</p> <p>- a.6 - Authorization to Place Into Production -- Does this include DATABASE updates such as modifying existing records or adding new records? Formal authorization approvals and advance documentation may be applicable to PLANNED software patches/system changes; however Emergency situations which are impeding power system operations and reliability may necessitate immediate changes without the luxury of time to gain formal testing and authorization. If Emergency actions are required, these should be acceptable with after-the-fact documentation without incurring non-compliance. For example, in that EMS systems model the real world network, some permutations may occur within the power system which has not occurred previously and therefore not modeled in previous testing criteria.</p>	<p>1301.a.2.ii - This does not include every piece of information within the entity. Only that information that is associated with critical cyber assets whose loss or compromise would have an impact on the bulk electric system. It is up to the individual entities to define their information categorization program.</p> <p>1301.a.5.iv - This section has been reworded to address business requirements.</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p>

Name	Company	Comments	Drafting Team Response
Ed Riley	CAISO	<p>1301.a.2 Change Information Protection to Information Protection Program to be aligned with the references within the measurement section. Remove "used by", the pertaining to is defined below.</p> <p>1301.a.2.i Remove "all", minimum requirements is defined. Disaster Recovery plans should be specifically identified as a minimum requirement.</p> <p>1301.a.2.ii The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.</p> <p>1301.a.2.iii "as defined by the individual entity" should be included after classification level to read "...classification level as defined by the individual entity."</p> <p>1301.a.3 Where is section 1.2?</p> <p>1301.a.5.i Remove "or used by".</p> <p>1301.a.5.iv Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.</p> <p>1301.b.1.ii Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".</p> <p>1301.b.2 To be consistent, change title to Information Protection Program.</p> <p>1301.b.1.5.i Seems to be speaking about critical cyber "information" but the last work refers to "assets." The last word in the sentence should be "information." This sentence could be reworded to make a clearer statement. Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>The review periods seem to be to often and don't seem to synchronize with each other in this section.</p> <p>1301.b.6 Remove the last line. The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>1301.d.3 This section should provide more clarification to identify the meaning of audit result which refers to compliance with the NERC 1300 Standard and not any other audit.</p>	<p>The drafting team disagrees. The title "Information Protection" is the same as the title in the measurements section. We will change the word "process" to read "program" in 1301.1.2</p> <p>Drafting team agrees and removes the word "used by or pertaining to " and substitutes "associated with" in 1301.1.2.</p> <p>1301.1.2.1 - Drafting team has changed the wording by removing "At a minimum" and replacing with "This includes". The word "all" should remain to be all inclusive of any information related to critical cyber assets.</p> <p>Added Disaster Recovery Plans as part of information identification 1301.1.2.1</p> <p>1301.1.2.2 Unauthenticated changed to unauthorized.</p> <p>1301.1.2.3 - Added the words "as defined by the individual entity" after classification level.</p> <p>1301.1.3 - Change reference 1.2 to read 1301.1.2</p> <p>1301.1.5 - Removed "used by or pertaining to" and replaced with "associated with".</p> <p>1301.1.5.3 - Replaced "Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised." with "Responsible entities shall define procedures to ensure that modification, suspension, or termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not put at significant risk."</p> <p>1301.2.1.2 - 1201.2.2 states "The responsible entity shall review the cyber security policy at least annually." This must remain as stated in 1200 standard.</p> <p>1301.2.1.2 Revised statement to read "The responsible entity shall review the cyber security policy as often as determined by the entity with a minimum review period not to exceed three years."</p> <p>1301.2.2 Statement answered in 1301.1.2</p>

Name	Company	Comments	Drafting Team Response
			<p>1301.2.5.1 - Changed "critical cyber information" to " critical cyber assets"</p> <p>1301.2.5.1 - changed statement to read "The responsible entity shall have a defined process that maintains a current list of designated personnel responsible to authorize access to critical cyber assets to reflect any change in status that affects the designated personnel's ability to authorize access to those critical cyber assets."</p> <p>Removed 2.5.2</p> <p>1301.2.6.1 changed to read "The responsible entity shall have a defined process that maintains a current list of designated personnel responsible for authorizing systems suitable for the production environment."</p> <p>Removed section 1301.2.6.2</p> <p>1301.4.3.4 changed from "Audit results and mitigation strategies..." to read "Documented review results of this standard and mitigation strategies..."</p>



Name	Company	Comments	Drafting Team Response
Ed Stein	FirstEnergy	<p>1301 Security Management Controls Section</p> <p>Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.</p> <p>Governance section, which requires entities to document structure for decision making at executive level.</p> <ul style="list-style-type: none"> <li>o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.</li> </ul> <p>Roles &amp; Responsibilities requiring participants to "maintain in its policy the defined roles &amp; responsibilities..."</p> <ul style="list-style-type: none"> <li>o If The Roles &amp; Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users...identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.</li> </ul> <p>Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing...and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "...change control documentation shall include records of test procedures, results of acceptance of successful completion...documentation shall verify that all changes to critical cyber assets were successfully tested...prior to being rolled into production..." Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate</p>	<p>The requirements of 1301 do not require a specific format of documentation only that the entity does document its processes. Most auditors will review your documentation to determine how it lines up with the requirements. Many of these requirements are expanded from 1200 and therefore should not introduce significant additional strain on organizations.</p> <p>1301 Security Management Controls requires a control structure to monitor and ensure compliance with this standard. As such, Governance does not reside with one person. Rather, Governance is part of the corporate culture.</p> <p>1.2 has been renumbered to read 1301.1.2</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>The FAQ was provided as the drafting team's explanation of some of the sections. It is not part of the standard and will not be incorporated into it. It is merely an aid.</p> <p>Access Revocation/Changes section has been re-worded to be more consistent throughout the document.</p> <p>The drafting team disagrees with removing the term "all information" primarily because it is up to each entity to determine what information relates to critical cyber assets.</p> <p>A minimum level of protection would be the minimum amount of processes and procedures in place to meet requirements and ensure that the entities critical cyber assets are reasonably protected from loss or compromise.</p> <p>Drafting team disagrees with limiting levels of noncompliance on level 4. Level 4 indicates that a company has done little to even begin to comply with the standard. However, these are not cumulative. Not having one of the requirements complete will not necessarily trigger a noncompliance.</p> <p>Access changes not being accomplished within 24 hours has been eliminated.</p>

Name	Company	Comments	Drafting Team Response
		<p>approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.</p> <p>NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "...entities to...identify controls...designate approving authorities that will formally authorize and document that a system has passed testing criteria....approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " ...assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that ..." testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.</p> <p>Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are. - 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</p> <p>Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."</p> <p>Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.</p> <p>Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles &amp; Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-</p>	

Name	Company	Comments	Drafting Team Response
		<p>compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles &amp; Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.</p> <p>Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.</p>	

Name	Company	Comments	Drafting Team Response
Francis Flynn	National Grid	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets."</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well."</p> <p>Change 1301.a.3 from;</p> <p>"...entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."</p> <p>The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.</p> <p>Change 1301.a.5.iv from;</p> <p>"Responsible entities shall define procedures to ensure that</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		<p>modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."</p> <p>to</p> <p>"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven business days for all other users of a change in user access status. All access revocations/changes must be authorized and documented."</p> <p>(Note: The 7 days would put this standard in line with the new FERC Order 2004b Standards of Conduct.)</p> <p>change 1301.b.5.i from;</p> <p>"5 days"</p> <p>to</p> <p>"7 calendar days"</p> <p>In 1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency.</p> <p>In 1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor</p> <p>In 1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii</p> <p>In 1301.c Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>In 1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>In 1301.e.2.iii, change from;</p>	<p>been designated but a formal process to validate and promote systems to production does not exist"</p> <p>1301.5.4.11 removed</p>

Name	Company	Comments	Drafting Team Response
		<p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p>	
		<p>to</p>	
		<p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or"</p>	
		<p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i. If kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p>	
		<p>In 1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days(should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p>	
		<p>National Grid believes that the concept of the Bulk Electric System and associated "definitions" may not be appropriate to capture the intent of the standard. National Grid suggests the substantive changes as shown below to address this issue which will also include a new concept of Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Gary Campbell		<p>1301</p> <p>The requirement is very large and should be consider to be divided into additional requirements. The complexity makes it difficult to focus on a particular subject matter in any great detail which would be helpful to the entity and CM</p> <p>Roles and Responsibilites:</p> <p>Why are we allowing roles and responsibilites to be defined by the entity? There will not be any consistency across the interconnection then.</p> <p>Measures:</p> <p>Many of the measures should be part of the requirements. In requirements, i believe you should be setting the minimum you want the entity to have in order to ensure protection of the cyber infastructure. Then a measure would be to " have the policy" or "have the policy reviewed in accordance with the requirement".</p> <p>Levels of Noncomplance</p> <p>There are to many or statements in the levels of non compliance and this is another reason to consider futher division of the requirement. In some parts, it seems the the requirements may be restated. An approach would be to state the requirements of procedures, processes or plans in the requirements section, designate in the measure section which requiremetns should be monitored by the CM and in the levels of compliance then assign levels of non-compliacne to the number of missing requirements</p> <p>Level 3</p> <p>Roles and Responsibilites are not clearly defined. I do not know what clearly defined means and what clearly defined for one person may not be the same for another individual.</p>	<p>Roles and Responsibilities need to be defined by each entity to closely follow their business processes and not an artificial one created by this standard. By allowing the entities to define this item themselves, it makes each defined role accountable for their actions and each role and responsibility auditable.</p> <p>Requirements state what needs to be done. Measures define how the requirement shall be measured.</p> <p>Levels of non-compliance - The drafting team disagrees that there are too many levels. Each level is defined to address each section of 1301.</p> <p>Level 3 - In most organizations, the Human Resources department has a definition of each job title (role) and the responsibilities for that job title. In the same respect, if you were hiring for a transmission operator position you would define the responsibilities of that position before you hired for it. The drafting team considers a role of "Transmission Operator" with responsibilties of "monitors the transmission of electricity" as not being clearly defined.</p>

Name	Company	Comments	Drafting Team Response
Greg Fraser	Manitoba Hydro	<p>In section 1301 (a) (2) (i) Identification: Replace...this must include access to procedures...with...this must include the procedures...Removing the word access makes it clearer that the documents and not the access is being protected since access is include below in (iii) Protection. In section 1301 (a) (2) (i) Identification: Should files, schematics, and data be included in the list of information types requiring identification or perhaps an FAQ could describe more about the type of information which require protection? In section 1301 (a) (2) (ii) Classification - suggest revising as follows to simplify and remove possible confusion: The responsible entity shall classify information based on the relative sensitivity of the information related to critical cyber assets. In section 1301 (a) (2) (iii) Protection, Change the word ...limitations... to... controls.</p>	<p>1301.a.2.1 change to "...this includes procedures,..."</p> <p>1301.a.2.i - Each entity will have to decide what information is critical cyber asset information and what is not. If the information is associated with or related to a critical cyber asset, then that information needs to be identified and protected.</p> <p>1301.a.2.ii - Drafting team disagrees. The suggested revision is to vague.</p> <p>1301.a.2.iii - Drafting team agrees. Changed.</p>



Name	Company	Comments	Drafting Team Response
Guy Zito	NPCC	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Jim Hiebert	WECC EMS WG	<p>Change Information Protection to Information Protection Program to be aligned with the references within the measurement section.</p> <p>1301.a.2.i Remove "all", minimum requirements is defined.</p> <p>1301.a.2.ii The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.</p> <p>1301.a.2.iii "as defined by the individual entity" should be included after classification level to read "...classification level as defined by the individual entity."</p> <p>1301.a.5 Remove "or used by".</p> <p>Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.</p> <p>1301.b.1.ii Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".</p> <p>1301.b.2 To be consistent, change title to Information Protection Program.</p> <p>1301.b.5 Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>The review periods seem to be to often and don't seem to synchronize with each other in this section.</p> <p>1301.b.6 Remove the last line. The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>Remove "used by", the pertaining to is defined below.</p>	<p>Drafting team disagrees - The section title "Information Protection" is identical to the one in the measurements section. Information Protection is used as a section heading to denote a program and controls for the protection of information.</p> <p>1301.a.2.i - Drafting team disagrees with removing the word "all". The statement following provides examples of types of information to include but is not and all inclusive or minimum requirements list.</p> <p>1301.a.2.ii - "Unauthenticated" changed to "unauthorized"</p> <p>1301.a.2.iii - Changed</p> <p>1301.a.5 - revised to state "associated with"</p> <p>1301.a.5.iv (Access/Revocation Changes) - Section has been reworded.</p> <p>1301.b.1.ii - Review cycle changed to state "not to exceed 3 years."</p> <p>1301.b.2 - See first response</p> <p>1301.b.5.i - Timeframe modified to be more in keeping with business needs.</p> <p>1301.b.6 - Section reworded and moved under governance.</p> <p>"...pertaining to or used by..." changed to "associated with"</p>

Name	Company	Comments	Drafting Team Response
Joanne Borrell	First Energy Services	<p>1301 Security Management Controls Section</p> <p>Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.</p> <p>Governance section, which requires entities to document structure for decision making at executive level.</p> <ul style="list-style-type: none"> <li>o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.</li> </ul> <p>Roles &amp; Responsibilities requiring participants to "maintain in its policy the defined roles &amp; responsibilities..."</p> <ul style="list-style-type: none"> <li>o If The Roles &amp; Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users...identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.</li> </ul> <p>Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing...and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "...change control documentation shall include records of test procedures, results of acceptance of successful completion...documentation shall verify that all changes to critical cyber assets were successfully tested...prior to being rolled into production..." Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate</p>	<p>The requirements of 1301 do not require a specific format of documentation only that the entity does document its processes. Most auditors will review your documentation to determine how it lines up with the requirements. Many of these requirements are expanded from 1200 and therefore should not introduce significant additional strain on organizations.</p> <p>1301 Security Management Controls requires a control structure to monitor and ensure compliance with this standard. As such, Governance does not reside with one person. Rather, Governance is part of the corporate culture.</p> <p>1.2 has been renumbered to read 1301.1.2</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>The FAQ was provided as the drafting team's explanation of some of the sections. It is not part of the standard and will not be incorporated into it. It is merely an aid.</p> <p>Access Revocation/Changes section has been re-worded to be more consistent throughout the document.</p> <p>The drafting team disagrees with removing the term "all information" primarily because it is up to each entity to determine what information relates to critical cyber assets.</p> <p>A minimum level of protection would be the minimum amount of processes and procedures in place to meet requirements and ensure that the entities critical cyber assets are reasonably protected from loss or compromise.</p> <p>Drafting team disagrees with limiting levels of noncompliance on level 4. Level 4 indicates that a company has done little to even begin to comply with the standard. However, these are not cumulative. Not having one of the requirements complete will not necessarily trigger a noncompliance.</p> <p>Access changes not being accomplished within 24 hours has been eliminated.</p>

Name	Company	Comments	Drafting Team Response
		<p>approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.</p> <p>NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "...entities to...identify controls...designate approving authorities that will formally authorize and document that a system has passed testing criteria....approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " ...assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that ..." testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.</p> <p>Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>Further on the subject of Access requirements, commentators stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website</p>	

Name	Company	Comments	Drafting Team Response
		<p>provided the following:</p> <p>"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence...."</p> <p>While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard.'" Since objections have not been addressed, NERC still needs to do this.</p> <p>Regarding requirements for updating access records, ABC recommends:</p> <p>(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <p>(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.</p> <p>(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.</p> <p>Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."</p> <p>Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.</p> <p>Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can</p>	

Name	Company	Comments	Drafting Team Response
		<p>trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles &amp; Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles &amp; Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.</p> <p>Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.</p>	



Name	Company	Comments	Drafting Team Response
John Blazeovitch	Exelon	<p>1301 Security Management Controls</p> <p>1301.b.1.iii Please explain how deviations and exemptions impact levels of noncompliance</p> <p>1301.a.5.iv This section requires termination of user access to critical cyber assets to be accomplished within 24 hours of a change in user status. We agree that access must be updated within 24 hours for cases where a person loses his/her access rights due to cause. The NRC allows three days for a favorable termination and this standard should not be more demanding than the highly regulated nuclear industry. We believe that routine administrative status changes should be managed within six business days.</p> <p>1301.b.5.i This section states that the list of designated personnel must be updated within five days. This timeframe is unclear and we recommend changing five days to five business days.</p>	<p>1301.2.1.3 - Deviations and exceptions to this standard in and of themselves do not impact levels of noncompliance. Not documenting these deviations/exceptions is what creates the noncompliance.</p> <p>1301.1.5.3 - Section has been re-worded to provide more flexibility. Section 1301.2.5.3 calls for access changes within 24 hours for suspension or termination for cause and 3 days for normal administrative changes.</p> <p>All references to days and months have been changed to reflect either calendar or business days and months.</p>

Name	Company	Comments	Drafting Team Response
John Hobbick	Consumers Energy	<p>1301 -- Security Management Controls</p> <p>2) Information Protection The first sentence of section (i) identification should have the word "all" removed, it is impossible to certify that ALL information is identified and protected. What is meant by maps? Is this maps of our electric system, maps of our buildings that contain the critical cyber assets, etc.</p> <p>5) Access Authorization The requirements in section IV Access Revocation / Changes needs to be made consistent with the other sections in the standard. The requirement should be 24 hours for cause, 5 days for other changes</p> <p>6) Authorization to Place Into Production Most of this section is redundant with 1306 Test Procedures and redundancy needs to be eliminated, in particular the requirements for redundant documentation.</p> <p>Levels of non-compliance, there are far too many (11) different items that can trigger a non-compliance item. At a minimum, remove the following items; (v) Executive management has not been engaged in the cyber security program (vi) No corporate governance program exists (viii) There is no authorizing authority to validate systems that are to be promoted to production</p>	<p>2) This only applies to information related to critical cyber assets. Not all information will be related to these assets. Maps changed to critical cyber network maps.</p> <p>5) Access Revocation section re-worded to permit the entities to define the processes that work best for their environments and protect their critical cyber assets.</p> <p>6) Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>Drafting team disagrees with comment that there are too many levels of non-compliance. The three sections cited (v) Executive management has not been engaged in the cyber security program (vi) No corporate governance program exists (viii) There is no authorizing authority to validate systems that are to be promoted to production are some of the most important items. Without engaging executive management, not having a corporate governance program and not having an authorizing authority almost guarantees that compliance with this standard will fail. Therefore, the drafting team will not remove these items.</p>

Name	Company	Comments	Drafting Team Response
Karl Tammer	ISO-RTO Council	<p>1301.a.2.i Disaster recovery plans should be specifically identified.</p> <p>1301.a.2.ii The use of "unauthenticated" personnel is anomalous to the rest of the document. "Unauthorized" is a better term. Even some authenticated personnel may not necessarily be authorized.</p> <p>The word "entity" should be "organization"</p> <p>1301.a.2.iii "as defined by the individual organizations" should be included after classification level, to read -- "...classification level as defined by the individual organizations."</p> <p>1301.b.5.i Seems to speak about critical cyber "information" but the last word refers to "assets". Should the last word in the sentence be "information"? This sentence should be made clearer.</p> <p>1305.d</p> <p>This section should provide clarification to indicate the meaning of audit result, which we believe means compliance with the NERC 1300 standard and not other audits.</p>	<p>1301.1.2.1 DR plans added</p> <p>1301.1.2.2 Change to "unauthorized"</p> <p>The word "entity" refers to more than just organizations and is the term used in the NERC functional model.</p> <p>1301.1.2.3 changed</p> <p>Critical cyber assets include critical cyber information. Therefore, "critical cyber information" changed to "critical cyber asset"</p> <p>The term "Audit" has been changed to "Documented review results"</p>

Name	Company	Comments	Drafting Team Response
Kathleen Goodman	ISO-NE	<p>1301 PREAMBLE:</p> <p>The role/description of "Monitoring," as presented in the FAQ should be added directly to the standard in 1301 as a governance requirement of the responsible entity. Reference FAQ page 2, sub-header Monitoring.</p> <p>(This is recognized to be different from the role of the NERC/Regional Compliance Monitor, which is defined independently.)</p> <p>1301 REQUIREMENTS:</p> <p>(2) Information Protection: Rewrite as: "...protection of critical information pertaining ... "</p> <p>(i) Identification - Disaster Recovery/Business Continuity plans should also be protected at a minimum</p> <p>(ii) Classification - The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.</p> <p>(iii) Protection - Where are differing classification levels defined?</p> <p>(3) Roles and Responsibilities Where is 1.2?</p> <p>(5.iv) 24-hour requirement is unrealistic in most cases. Requirement should be within 24 hours for facility and remote access for terminations with cause or other disciplinary action. Next Business Day for all other access.</p> <p>(6) Authorization to Place Into Production Needs to be worded to be specific to placing Critical Cyber Asserts Into Production.</p> <p>1301 MEASURES:</p> <p>(2) Information Protection: Remove the use of the word "security" and "secure" and only use "protection" or "protect."</p> <p>(5) Access Authorization --</p> <p>(i) Seems to speak about critical cyber "information" but the last word refers to "assets." Should the last word in the sentence be "information?" Also, change 5 days to seven days.</p> <p>(ii) Reviewing of user access rights every quarter is excessive. We recommend annually on revalidation.</p> <p>(6) Authorization to Place Into Production Needs to be worded to be specific to placing Critical Cyber Asserts Into</p>	<p>The FAQ was provided as an aid only and will not be part of the standard.</p> <p>1301.a.2 - Reworded as "...protection of critical information associated with..."</p> <p>1301.a.2.i - Reworded to include D/R plans</p> <p>1301.a.2.ii - Changed unauthenticated to unauthorized</p> <p>1301.a.2.iii - Each entity will set its own categories to define the sensitivity levels of information. Examples of some common levels are "Sensitive", "Confidential", "Public", etc.</p> <p>1301.a.3 - reworded to read 1301.1.2</p> <p>1301.a.5.iv - Timeframe reworded to better address business needs.</p> <p>1301.a.6 - Section reworded and moved under 1301.a.4</p> <p>1301.b.2 - Drafting team disagrees. Terminology is in keeping with this Cyber Security Standard.</p> <p>1301.b.5.i - reworded and timeframe changed to "maintain a current list"</p> <p>1301.b.5.ii - Changed review to annually.</p> <p>1301.b.6 - Reworded and moved under 1301.b.4</p> <p>1301.d.2 - At this point, all data related to this standard. Compliance reports, internal assessments, etc.</p> <p>1301.d.3.iv - Changed "audit" to "Documented review results"</p> <p>1301.e.1.3 - What this means is that you had a deviation or exception to the standard and/or your written cyber security policy and you did not document it within a 30 calendar day period.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person</p>

Name	Company	Comments	Drafting Team Response
		<p>Production. Also, change 48 hours to seven days.</p> <p>1301 Compliance Monitoring</p> <p>(2) identify specific data that is kept for three years This needs to be clarified in all sections 1301 through 1308.</p> <p>(3.iv) This should provide clarification to indicate the meaning of audit results which we believe means compliance with the NERC 1300 standard and not other audits. This needs to be clarified in all sections 1301 through 1308.</p> <p>1301 Levels Noncompliance</p> <p>(1.iii) Request clarification on "30 days of the deviation." Also, please explain the difference between "deviation" and "exception." This does not match the FAQ 1301 Question 4.</p>	<p>designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p>

Name	Company	Comments	Drafting Team Response
Ken Goldsmith	Alliant Energy	<p>1301 Security Management Controls</p> <p>Article a-5-iv, Access Revocation Changes should be within 24 hours for cause only. It should not attempt to define when it is removed for other reasons. This should be a documented procedure within the organization regarding review and revocation of access.</p> <p>Article a-6, Authorization to Place Into Production does not seem to belong in this section and may fit better in 1306 where testing is addressed.</p>	<p>1301.1.5.3 Access Revocation Changes - Changed to "Responsible entities shall define procedures to ensure that modification, suspension, or termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not put at significant risk." Section 1301.2.5.3 specifies changes to be made within 24 hours for suspension or termination for cause and within 3 days for all other administrative changes.</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p>

Name	Company	Comments	Drafting Team Response
Larry Brown	EEI Security Committee	<p>Section 1301</p> <p>(a)(3)(1st parag.) -- The proposed language makes it appear that only one responsible member of senior management shall be chosen from each responsible entity. This ignores that there are major operating subdivisions. Revise the operative phrase to read: "shall assign at least one member of senior management, consistent with the corporate structure and division of responsibilities, with responsibility for."</p> <p>(a)(5)(iv) -- The 24-hour rule for change/termination of access is too short for general use, and is inconsistent with the limits established in 1306(b)(2). This should only apply to dismissals "for cause" -- routine transfers should allow at least three days, ideally five, and perhaps even seven days depending on circumstances and other relevant corporate policy. Even the NRC allows three days for a "favorable" termination, and we understand that FERC allows seven days regarding market-access related changes. Further, Sarbanes-Oxley requirements for corporate governance leave the time to address favorable termination up to the company. Moreover, for some equipment 24 hours is not realistic, as that equipment may require a manual visit (e.g., at substations) or call-up.</p> <p>(a)(6) -- This subsection should be moved to 1306 -- it fits more into that subject area (revise and renumber format).</p> <p>(d)(1) -- What is meant by "onsite reviews every three years"? The period is acceptable if such a review is part of the triennial NERC audit -- it is far too frequent if to be conducted by hired independent auditors.</p>	<p>1301.a.3 - Drafting team disagrees. If more than one member of senior management is responsible for the program, then who would be accountable? Most organizations have only one CEO, CIO, COO, etc. These individuals are responsible for their particular piece of the organization. They accomplish their goals through delegation. The same thing can be applied here. The individual chosen can delegate some of the responsibilities. However, it is their signature that is applied to the self-certification form attesting to the entities compliance with this standard.</p> <p>130.a.5.iv - Section has been rewritten to address business needs.</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>1301.d.1 - The onsite audits are conducted by the compliance monitor who can be from NERC or the regional authority. This is not implying an audit conducted by and outside auditing firm such as KPMG.</p>

Name	Company	Comments	Drafting Team Response
Larry Conrad	Cinergy	<p>1301 Security Management Controls Section</p> <p>Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, Cinergy recommends section such as those listed below be eliminated or modified.</p> <p>Governance section, which requires entities to document structure for decision making at executive level.</p> <ul style="list-style-type: none"> <li>o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.</li> </ul> <p>Roles &amp; Responsibilities requiring participants to "maintain in its policy the defined roles &amp; responsibilities..."</p> <ul style="list-style-type: none"> <li>o If The Roles &amp; Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users...identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.</li> </ul> <p>Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing...and document that a system has passed testing criteria." Cinergy agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "...change control documentation shall include records of test procedures, results of acceptance of successful completion...documentation shall verify that all changes to critical cyber assets were successfully tested...prior to being rolled into production..." Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate</p>	<p>The requirements of 1301 do not require a specific format of documentation only that the entity does document its processes. Most auditors will review your documentation to determine how it lines up with the requirements. Many of these requirements are expanded from 1200 and therefore should not introduce significant additional strain on organizations.</p> <p>1301 Security Management Controls requires a control structure to monitor and ensure compliance with this standard. As such, Governance does not reside with one person. Rather, Governance is part of the corporate culture.</p> <p>1.2 has been renumbered to read 1301.1.2</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>The FAQ was provided as the drafting team's explanation of some of the sections. It is not part of the standard and will not be incorporated into it. It is merely an aid.</p> <p>Access Revocation/Changes section has been re-worded to be more consistent throughout the document.</p> <p>The drafting team disagrees with removing the term "all information" primarily because it is up to each entity to determine what information relates to critical cyber assets.</p> <p>A minimum level of protection would be the minimum amount of processes and procedures in place to meet requirements and ensure that the entities critical cyber assets are reasonably protected from loss or compromise.</p> <p>Drafting team disagrees with limiting levels of noncompliance on level 4. Level 4 indicates that a company has done little to even begin to comply with the standard. However, these are not cumulative. Not having one of the requirements complete will not necessarily trigger a noncompliance.</p> <p>Access changes not being accomplished within 24 hours has been eliminated.</p>



Name	Company	Comments	Drafting Team Response
		<p>approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.</p> <p>NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "...entities to...identify controls...designate approving authorities that will formally authorize and document that a system has passed testing criteria....approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " ...assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that ..." testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. Cinergy recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.</p> <p>Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>Further on the subject of Access requirements, commentators stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website</p>	

Name	Company	Comments	Drafting Team Response
		<p>provided the following:</p> <p>"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence...."</p> <p>While Cinergy acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard.'" Since objections have not been addressed, NERC still needs to do this.</p> <p>Regarding requirements for updating access records, Cinergy recommends:</p> <p>(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <p>(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.</p> <p>(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.</p> <p>Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. Cinergy recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."</p> <p>Page 3: Cinergy seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.</p> <p>Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can</p>	

Name	Company	Comments	Drafting Team Response
		<p>trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles &amp; Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles &amp; Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.</p> <p>Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.</p>	

Name	Company	Comments	Drafting Team Response
Laurent Webber	WAPA	<p>Under 1301(a)(3), the sentence that reads, "This person must authorize any deviation or exception from the requirements of this standard," should be changed to read, "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation."</p> <p>Under 1301(d)(3)(ii), remove the word "and" at the end of the sentence.</p> <p>Under 1301(e)(1), what is the difference between (iv) and (v)?</p>	<p>1301(a)(3) - Drafting team disagrees. The standard already requires that the person responsible for the cyber security program be documented by listing the person's name, etc. Listed under section 1301.2.3.2. Also, provision has been added to allow for the senior manager to authorize a delegate to review and authorize deviations or exceptions.</p> <p>1301(d)(3)(ii) Word "and" removed from end of sentence.</p> <p>130.1.5.1.4 and .5 - No difference. 1301.5.1.5 removed.</p>

Name	Company	Comments	Drafting Team Response
Linda Campbell	FRCC	<p>Section 1301 Security Mangement Controls</p> <p>(a) (2) (i) Identification - "all information related to critical cyber assets" seems a bit broad. In (5) (i) you limit the information that the "access process" needs to deal with to "that information whose compromise could impact. reliability and/or availability...". We would like the wording of (a) (2) (i) to be similar:</p> <p>The responsible entity shall identify all information pertaining to or used by critical cyber assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible, regardless of media type.</p> <p>(a)(2)(iii) --Information Classification</p> <p>Under generally accepted security best practices, an information classification program typically entails the classification of information into multiple categories (public, internal, confidential, top secret, etc), with separate handling procedures for security, retention, destruction etc. A program such as this can be very resource intensive and overly burdensome, which we do not feel should be the intent of this standard. This standard seems to be addressing only the protection aspect of such a program, and all information related to critical cyber assets (whose compromise would impact reliability, etc.) would likely fall into a single category as it relates to the protection of information. The intent of the standard should be to identify and protect such information, and we recommend that the use of a classification system or some other means to protect the information should be left up to the individual organization. Measures (b) (2) (iii) and (iv) would go away if this is changed.</p> <p>(a)(3) -- The terms, deviation and exception (used in paragraph 1), are unclear in the standard and in the FAQ. Is a deviation where an organization has implemented a compensating control when unable to meet the specific requirements of the standard, or when an organization has opted not to meet the requirements in the standard and accepts the risk related to this omission? If an organization has a deviation by using compensating controls, they might be considered in compliance, but if they have opted not to follow the standard and accept the risk, they might be considered non-compliant. This needs to be clarified, perhaps in the definitions, and made very clear when a deviation, exception, or exemption is acceptable from a compliance standpoint. See comment in the definitions section above.</p> <p>The documentation required to be kept of any deviation of exception might be sensitive in nature and must be given some level of confidentiality, especially given the Sunshine Law in Florida.</p>	Please see responses to Paul McClay.

Name	Company	Comments	Drafting Team Response
		<p>(a) (4) Governance -- This seems to be redundant.. The senior management official named in (a) (3) has the responsibility to lead the implementation and the policy (a) (1) to manage governance. While the FAQ is helpful in what the senior management official might do, the standard is not and should not be prescriptive for how this is done. The governance requirement doesn't seem to add any value. Recommend deleting this statement and the associated measure (b) (4).</p>	
		<p>(a) (5) (ii) Not sure if the sentence, "all access authorizations must be documented", is saying you need to "document who may authorize access" (which would be redundant, since a list is a document) or that the accesses the authorizer permits need to be documented, in which case this sentence seems to belong better in (a) (5) (i) as a requirement of the process.</p>	
		<p>(a) (5) (iv) Suggest wording change to indicate 24 hours applies only to "unfriendly terminations" not all changes. 3-5 days seems to be more appropriate for "friendly separations" and transfers.</p>	
		<p>(a) (6) Authorization to Place into Production -- this paragraph starts with the requirement to identify controls for testing and "assessment" (whatever that means) of new or replacement systems... The 1301 section is called security management controls -- testing of new systems doesn't seem to fit in this section unless you are specifically referring to testing of security for new or replacement systems only. Please clarify the wording.</p>	
		<p>This section also states that an approving authority must authorize and document that a system has passed "testing criteria". And ends with "the approving authority shall verify system meets minimal security configuration standards". What testing criteria does this refer to? Are they the controls for testing or something different? Is the intent of this section to ensure the system meets minimum security standards, that functionality is tested, that there are testing controls or all of the above? The test procedures referred to in 1306 are clearly for testing information security; are these same procedures? The intent in this section is unclear. Section (a) (6) should be reworded to clarify.</p>	
		<p>(b) (1) Cyber Security Policy Measures The measures refer to deviations, yet the requirements do not cover deviations in the policy section (a) (1) but rather in the roles and responsibilities (a) (3) section. Are we to document deviations and exceptions to the organization's policy or to the cyber standard requirements? The requirements and measures should address deviations in the same sections.</p>	

Name	Company	Comments	Drafting Team Response
		<p>(b)(1)(iii) &amp; (b)(1)(iv) These two sections deal with 1301(a)(3) Roles and Responsibilities and should be moved to 1301(b)(3). Then the parallel between the Requirements, Measures, and Levels of Noncompliance will match.</p> <p>(b)(1)(iv) Who will review the authorized deviations or exemptions? The senior management official is the person who authorizes the deviations/exemptions; therefore someone senior to him/her should be responsible to review.</p> <p>(b) (2) Information Protection Measures -- In (i) and (ii) delete the word "security" here or add to the requirements section- it was not used there. What is the difference between "reviewing" (i) the program annually and "assessing (ii) the program for compliance annually? Do you really need two measures here? How is "measure" (iii) different than the requirement to "document and implement a process.."</p> <p>(b)(3)(iii) What changes must be documented within 30 days of the effective date? The Roles and Responsibilities section has several areas that are changeable:</p> <ol style="list-style-type: none"> <li>1. The senior management official could be changed</li> <li>2. Deviations or exemptions can be added/deleted/changed.</li> <li>3. Roles and responsibilities can be changed.</li> </ol> <p>(b)(3)(iv) Who will review the Roles and Responsibilities? The senior management official is the person who may or may not have defined the Roles and Responsibilities.</p> <p>(b) (5) (iii) Appears to be a requirement versus a measure. Suggest moving to (a) (5) (ii)</p> <p>(b) (6) (iii) What needs to be on the list appears to be a requirement versus a measure. Suggest moving to the requirements. It indicates changes to this list need to be documented in 48 hours; 5 days (such as for (b) (5) (i)) seems more reasonable and consistent.</p> <p>(d)(1) Who would be able to levy a complaint that would warrant an investigation?</p> <p>(d) (3) (iv) Compliance monitoring process -- This section is the first time use of the phrase "Audit and mitigation strategies" and "Audit results" appears. If this is referring to documentation of the information protection program review (or assessment if those are different), then wording needs to be consistent. Also refers here to "information</p>	

Name	Company	Comments	Drafting Team Response
		<p>protection security program" -- see comment related to (b) (2) above.</p> <p>(e) (1)-- Level 1 Non compliance --</p> <p>(iii) Suggest you change "deviations to policy" to "deviations from requirements"</p> <p>(e)(1)(iii) The time requirement is not clearly stated in section 1301(b)(3)(iii). Also, "deviations" are explained under the Roles &amp; Responsibilities section of the standard, not the policy. This area will need to be clarified.</p> <p>(iv) and (v) - refers here to "information protection security program" and separates review and assessment -- see comments related to (b) (2)</p> <p>(vi) seems redundant to the above.. Are the processes different than the "program"?</p> <p>(e)(2) Noncompliance for deviations/exemptions is not mentioned in this section.</p> <p>(e) (2) (iii) -- "formal process to validate and promote systems to production" - this "formal process" is not specified in the requirements</p> <p>(a) (6) -- only that you identify controls and have an approving authority. Same for (e) (3) (iv)</p> <p>(e)(2)(iv) Measures section 1301(b)(5)(ii) states review should be at least once per quarter.</p> <p>(e)(4) Noncompliance for deviations/exemptions is not mentioned in this section.</p> <p>(e)(4)(v) How would executive management's engagement be measured? And shouldn't that measurement be stated in the measures section?</p> <p>(e) (4) (xi) "Access revocations and change not accomplished within 24 hours." 3-5 days seems to be more appropriate for "friendly separations" and transfers. See comment on (a) (5) (iv).</p>	



Name	Company	Comments	Drafting Team Response
Linda Nappier	Ameren	1301 (a) (5) (iv) Access Revocation/Changes -- The time limit of 24 hours for modifications to user access changes conflicts with 1306 (b) (2). The latter section allows five days for modifications to user access changes. The five day limit is preferable to us.	1301.a.5.iv - Section has been re-worded to allow entities to determine what is appropriate in accordance with completed risk assessments that the entity has performed.

Name	Company	Comments	Drafting Team Response
Lloyd Linke	WAPA - MAPP	Under 1301 (a) (3), the sentence that says "This person must authorize any deviation or exception from the requirements of this standard." should be changed to read "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation."	Drafting team disagrees. The standard already requires that the person responsible for the cyber security program be documented by listing the person's name, etc. Listed under section 1301.2.3.2. Also, provision has been added to allow for the senior manager to authorize a delegate to review and authorize deviations or exceptions.

Name	Company	Comments	Drafting Team Response
Lloyd Linke	WAPA - MAPP	Under 1301 (d) (3) (ii), remove the word "and" at the end of the sentence.	1301.4.3.2 - removed the word "and" at the end of the sentence
		Under 1301 (e) (1). What is the difference between (iv) and (v)?	1301.5.1.4 and .5 - no difference. 1301.5.1.5 removed.

Name	Company	Comments	Drafting Team Response
Lyman Schaeffer	Pacific Gas & Electric	<p>Section 1301: Security Management Controls</p> <p>The section calls for a Senior Management Person to ensure compliance with the standard. Given the makeup of most companies, this should more logically be a shared responsibility between Generation, T&amp;D, and IT. Does one person have to be designated or can this be shared?</p> <p>The standard also refers to a "compliance monitor," but provides no additional detail as to who that person should be. Can this be the company's auditors? Must it be an outside party? Clarity will be required at some point.</p>	<p>There must be one person designated (Senior Management person) per the standard. This person is the one who signs the self-compliance form that is submitted to NERC. The act of ensuring compliance can be shared but only one person is ultimately responsible for the program.</p> <p>The "compliance monitor" has typically been at the regional level. It is the person from your region or from NERC that can audit you for compliance with this standard.</p>

Name	Company	Comments	Drafting Team Response
Paul McClay	Tampa Electric Company	<p>Section 1301 Security Mangement Controls</p> <p>(a) (2) (i) Identification - "all information related to critical cyber assets" seems a bit broad. In (5) (i) you limit the information that the "access process" needs to deal with to "that information whose compromise could impact. reliability and/or availability...". We would like the wording of (a) (2) (i) to be similar:</p> <p>The responsible entity shall identify all information pertaining to or used by critical cyber assets whose compromise could impact the reliability and/or availability of the bulk electric system for which the entity is responsible, regardless of media type.</p> <p>(a)(2)(iii) -- Information Classification</p> <p>Under generally accepted security best practices, an information classification program typically entails the classification of information into multiple categories (public, internal, confidential, top secret, etc), with separate handling procedures for security, retention, destruction etc. A program such as this can be very resource intensive and overly burdensome, which we do not feel should be the intent of this standard. This standard seems to be addressing only the protection aspect of such a program, and all information related to critical cyber assets (whose compromise would impact reliability, etc.) would likely fall into a single category as it relates to the protection of information. The intent of the standard should be to identify and protect such information, and we recommend that the use of a classification system or some other means to protect the information should be left up to the individual organization. Measures (b) (2) (iii) and (iv) would go away if this is changed.</p> <p>(a)(3) -- The terms, deviation and exception (used in paragraph 1), are unclear in the standard and in the FAQ. Is a deviation where an organization has implemented a compensating control when unable to meet the specific requirements of the standard, or when an organization has opted not to meet the requirements in the standard and accepts the risk related to this omission? If an organization has a deviation by using compensating controls, they might be considered in compliance, but if they have opted not to follow the standard and accept the risk, they might be considered non-compliant. This needs to be clarified, perhaps in the definitions, and made very clear when a deviation, exception, or exemption is acceptable from a compliance standpoint. See comment in the definitions section above.</p> <p>(a) (4) Governance -- This seems to be redundant. The senior management official named in (a) (3) has the responsibility to lead the implementation and the policy (a) (1) to manage governance. While the FAQ is helpful in what the senior management official might do, the</p>	<p>1301.a.2.i - Section has been reworded</p> <p>1301.a.2.iii - Drafting team disagrees. The purpose of categorizing the information is to not only identify what is critical cyber information but to also aid personnel in determining what is to be protected. By having a standardized methodology, we accomplish two things. We minimize the amount of information that would be considered critical cyber asset information and we ensure that all personnel can tell the difference between what is and is not company sensitive information.</p> <p>1301.a.3 - A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.a.4 - Drafting team disagrees with eliminating the section. The section has been reworded.</p> <p>1301.a.5.ii - Moved to 1301.a.5.i</p> <p>1301.a.5.iv - Timeframes adjusted to better address business needs.</p> <p>1301.a.6 - Reworded and moved under 1301.a.4 Governance</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>1301.b.1 - Deviations are considered to be any time you are unable to fully comply with a requirement of this policy or your written cyber security standard. These deviations must be documented. The same goes for exceptions.</p> <p>1301.b.2 - Drafting team disagrees. The word "security" as it is used here, describes the program designed to protect your critical information that is associated with your critical cyber</p>

Name	Company	Comments	Drafting Team Response
		standard is not and should not be prescriptive for how this is done. The governance requirement doesn't seem to add any value. Recommend deleting this statement and the associated measure (b) (4).	assets. 1301.b.5.iii - Drafting team disagree. It is a measure.
		(a) (5) (ii) Not sure if the sentence, "all access authorizations must be documented", is saying you need to "document who may authorize access" (which would be redundant, since a list is a document) or that the accesses the authorizer permits need to be documented, in which case this sentence seems to belong better in (a) (5) (i) as a requirement of the process.	1301.b.6.iii - Drafting team disagrees. This is a measure. 1301.d.3.iv - Changed the word "audit" to Documented review results". Also, see response for 1301.b.2
		(a) (5) (iv) Suggest wording change to indicate 24 hours applies only to "unfriendly terminations" not all changes. 3-5 days seems to be more appropriate for "friendly separations" and transfers.	1301.e.1.iii - Changed to read "Deviations from requirements or written cyber security policy..." 1301.e.1.iv and v - See response for 1301.b.2
		(a) (6) Authorization to Place into Production -- this paragraph starts with the requirement to identify controls for testing and "assessment" (whatever that means) of new or replacement systems... The 1301 section is called security management controls -- testing of new systems doesn't seem to fit in this section unless you are specifically referring to testing of security for new or replacement systems only. Please clarify the wording.	1301.e.1.vi - A process is the "how" something is done. For example, you may have a process that standardized the method by which new users are set up on your network. The "program" encompasses all the processes and procedures that help to make up that program. An Information security protection program would have processes and procedures to help ensure the confidentiality of the information addressed by the program.
		This section also states that an approving authority must authorize and document that a system has passed "testing criteria". And ends with "the approving authority shall verify system meets minimal security configuration standards". What testing criteria does this refer to? Are they the controls for testing or something different? Is the intent of this section to ensure the system meets minimum security standards, that functionality is tested, that there are testing controls or all of the above? The test procedures referred to in 1306 are clearly for testing information security; are these same procedures? The intent in this section is unclear. Section (a) (6) should be reworded to clarify.	1301.e.2.iii - Reworded 1301.e.4.xi - Removed from standard
		(b) (1) Cyber Security Policy Measures The measures refer to deviations, yet the requirements do not cover deviations in the policy section (a) (1) but rather in the roles and responsibilities (a) (3) section. Are we to document deviations and exceptions to the organization's policy or to the cyber standard requirements? The requirements and measures should address deviations in the same sections.	
		(b) (2) Information Protection Measures -- In (i) and (ii) delete the word "security" here or add to the requirements section- it was not used there. What is the difference between "reviewing" (i) the program	

Name	Company	Comments	Drafting Team Response
		<p>annually and "assessing (ii) the program for compliance annually? Do you really need two measures here? How is "measure" (iii) different than the requirement to "document and implement a process.."</p> <p>(b) (5) (iii) Appears to be a requirement versus a measure. Suggest moving to (a) (5) (ii)</p> <p>(b) (6) (iii) What needs to be on the list appears to be a requirement versus a measure. Suggest moving to the requirements. It indicates changes to this list need to be documented in 48 hours; 5 days (such as for (b) (5) (i)) seems more reasonable and consistent.</p> <p>(d) (3) (iv) Compliance monitoring process -- This section is the first time use of the phrase "Audit and mitigation strategies" and "Audit results" appears. If this is referring to documentation of the information protection program review (or assessment if those are different), then wording needs to be consistent. Also refers here to "information protection security program" -- see comment related to (b) (2) above.</p> <p>(e) (1)-- Level 1 Non compliance --</p> <p>(iii) Suggest you change "deviations to policy" to "deviations from requirements"</p> <p>(iv) and (v) - refers here to "information protection security program" and separates review and assessment -- see comments related to (b) (2)</p> <p>(vi) seems redundant to the above.. Are the processes different than the "program"?</p> <p>(e) (2) (iii) -- "formal process to validate and promote systems to production" - this "formal process" is not specified in the requirements</p> <p>(a) (6) -- only that you identify controls and have an approving authority. Same for (e) (3) (iv)</p> <p>(e) (4) (xi) "Access revocations and change not accomplished within 24 hours." 3-5 days seems to be more appropriate for "friendly separations" and transfers. See comment on (a) (5) (iv).</p>	

Name	Company	Comments	Drafting Team Response
Pedro Modia	Florida Power and Light	<p>1301.a.3 - The aforementioned mandate is far too prescriptive in that defining roles and responsibilities can become extensive over time as both roles and responsibilities change over time. It is suggested that this section be either clarified or stricken from the standard.</p> <p>1301.a.5.ii - Remove wording - Logical or physical access to critical cyber assets may only be authorized by the personnel responsible to authorize access to those assets.</p> <p>1301.a.5.iv - change From</p> <p>Responsible entities shall define procedures to ensure that modification, suspension, or termination of user access to critical cyber assets is accomplished subsequent to a change in user access status. All access revocations/changes must be authorized and documented.</p> <p>To</p> <p>Responsible entities shall define procedures to ensure that modification, Suspension for cause, and termination for cause of user access to critical cyber assets is accomplished within 24 hours of a change in user access status, when it is determined that the change was for cause, otherwise the revocation must be completed within 5 working days. All access revocations/changes must be authorized and documented.</p> <p>1301.a.6 - Responsible entities shall identify the controls for testing and assessment of new or replacement systems and software patches/changes.</p> <p>Delete - Responsible entities shall designate approving authorities that will formally authorize and document that a system has passed testing criteria. The approving authority shall be responsible for verifying that a system meets minimal security configuration standards as stated in 1304 and 1306 of this standard prior to the system being promoted to operate in a production environment. [This is not a realistic and practical approach to testing. A sound well established process should suffice rather than the aforementioned "formal authorization" method.]</p> <p>1301.b.1.iii - (iii) The responsible entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official responsible for the cyber security program.</p>	<p>1301.a.3 - The drafting team disagrees and feels that most job descriptions and information in HR databases should provide sufficient information to satisfy this requirement.</p> <p>1301.a.5.ii - Drafting team disagrees. Someone must be designated to approve a request for access to a critical cyber asset both physically and logically. Example would be access to an operations center and access to a SCADA systems. A grid operator would be an example of someone needing both physical and logical access.</p> <p>1301.a.5.iv - Section reworded</p> <p>1301.a.6 - Section reworded and moved under section 1301.a.4 Governance</p> <p>1301.b.1.iii - A deviation or exception to a requirement is documented to provide information as why a particular requirement cannot be met. "We don't have the time or resources" would not be an acceptable deviation. A deviation of "The person responsible for the cyber security program resigned as of &lt;date&gt;. We have designated an interim person to oversee the program until a replacement can be found. We expect to have a replacement person for this position within 120 days of this deviation." would be an acceptable deviation from both requirements and policy.</p> <p>The above is an example only. Once this standard has been approved by the ballot body, NERC would have to ultimately determine what would be an acceptable deviation through their compliance monitors.</p> <p>1301.b.1.iv - Exceptions/ deviations are typically time bound as in when you will be able to meet the requirement. What mitigating strategy you have in place would also be part of any documentation for this. While the standard does not specify a requirement that entities make all their documented exceptions/deviations time bound, it would make sense that each entity would want to do this anyway in order to be able to protect themselves from being too far out of compliance. The drafting team feels that adding this language to the standard would be overstating the obvious.</p> <p>1301.b.3.ii - Changed</p>



Name	Company	Comments	Drafting Team Response
		[Who has the final authority on exemptions or deviations? Is it the entity itself or NERC?]	1301.b.3.iii - Changed
		1301.b.1.iv - Add words at end of sentence - should such extensions be time sensitive.	1301.b.3.iv - Drafting team disagrees. Annual review of roles and responsibilities ensures that a system of security checks and balances is maintained and that each person has only the access that they require to do their job.
		1301.b.3.ii - Specify the "work" address of the senior management official.	1301.b.4 - Reworded
		1301.b.3.iii - Change From Changes must be documented within 30 days of the effective date.	1301.b.5.i - Reworded to address timeframes that are more in line with business practices.
		To Changes to the current senior management official must be documented within 30 days of the effective date.	1301.b.5.iii - Drafting team disagrees. Entities need to keep a list of personnel who have the responsibility and are authorized to allow access to the systems and/or buildings they are responsible for. This provides accountability and precludes just "anyone" from requesting access to a system or facility they have no business need to access.
		1301.b.3.iv - Delete - The responsible entity shall review the roles and responsibilities of critical cyber asset owners, custodians, and users at least annually.	1301.b.5.iv - Removed word "periodically"
		1301.b.4 Governance [This area needs further clarification as the its purpose is unclear]	1301.b.5.v - Reworded
		1301.b.5.i - Change From The responsible entity shall update the list of designated personnel responsible to authorize access to critical cyber information within five days of any change in status that affects the designated personnel's ability to authorize access to those critical cyber assets.	1301.b.6 - Reworded and moved under 1301.b.4
		To Access shall be granted to users and/or custodians of critical cyber assets by management or its designee as required by normal business needs. The granting of such access shall be in accordance to the entities procedure for granting access rights.	1301.d - The term investigations simply means "A detailed inquiry or systematic examination" or more simply, "to look into". A complaint could be from another entity, business, etc. A filed complaint that indicated a lapse in compliance with this standard would warrant an investigation to determine if the complaint had merit. This allows the compliance monitor to conduct an unscheduled, on-site review for compliance to these requirements. The extent to which the compliance monitor would conduct this review will need to be addressed at a later date with the organization responsible for compliance monitoring.
		1301.b.5.iii - Delete - The list of designated personnel responsible to authorize access to critical cyber information shall identify each designated person by name, title, phone, address, date of designation, and list of systems/applications they are responsible to authorize access for.	1301.d.3.ii - Changed
		1301.b.5.iv - Remove word "periodically"	

Name	Company	Comments	Drafting Team Response
		<p>1301.b.5.v - Change</p> <p>From</p> <p>The responsible entity shall review user access rights every quarter to confirm access is still required.</p> <p>To</p> <p>The responsible entity shall review user access rights annually or upon changes "due for cause", to confirm access is still required.</p> <p>1301.b.6 - Delete Section - (6) Authorization to Place Into Production</p> <p>1301.d - (d) Compliance Monitoring Process</p> <p>[Further clarification is required in regards to "investigations upon complaint." How intrusive are these investigation, and what would predicate such investigations?]</p> <p>1301.d.3.ii - Specify "work" address.</p>	

Name	Company	Comments	Drafting Team Response
Pete Henderson	IMO	<p>1301 Security Management Controls (a) Requirements (5) - Access Authorization Re (ii) Authorizing Access: If, as per 1301 (a) (5) (i) there is a process for access management which is instituted, then subsection (ii) is redundant.</p> <p>As written, subsection (ii) does not appear to contemplate an access authorization scheme which allows access based on role. Rather, it assumes an authorization scheme based on name. This is overly prescriptive.</p> <p>(b) Measures (5) - Access Authorization Similar to the comment on Subsection 1301 (a) (5) (ii) above, this subsection does not appear to contemplate an access authorization scheme which allows access based on role. Rather, it assumes an authorization scheme based on name. This is overly prescriptive</p>	<p>1301.a.5.i and ii - Drafting team disagrees. Access authorizers and access review does not assume any particular access control schema. While a designated authorizer can authorize access to a particular critical cyber asset, this access must be reviewed to ensure that those individuals granted access do not have more access than required. These two sections complement one another.</p> <p>1305.b.5 - refer to response above.</p>

Name	Company	Comments	Drafting Team Response
Phil Sobol	SPP CIPWG	<p>1301, (a), (5), (iv) The 24 hour requirement to change access status in all situations seems unnecessary. The 24 hour rule makes sense if you have termination for cause. But 72 hours would seem more appropriate for the routine situations.</p> <p>The Governance requirement in 1301 is not very clear.</p> <p>1301 The additional requirements constitute a significant investment in processes, standards and procedures in general areas.</p>	<p>1301.a.5.iv - Specific Timeframes removed</p> <p>Governance section has been re-worded</p> <p>NERC had stated early on in the development of the 1200 Urgent Action that NERC would be "raising the bar" with the drafting of the 1300 standard. We are drafting an implementation schedule that should ease the implementation of this standard.</p>

Name	Company	Comments	Drafting Team Response
Ray A'Brial	CHGE	<p>Request clarification on what information is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets.</p> <p>to</p> <p>The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets. (CHGE's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information.</p> <p>to</p> <p>The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well. (CHGE's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>1301.a.3 Needs clarification.</p> <p>Change 1301.a.3 from; ...entity's implementation of... to ...entity's implementation and adherence of...(CHGE's participating members believe it is important to stress that not only is it important to implement this Standard but to adhere to it as well.</p> <p>1301.a.3 - shall assign a member of senior management. needs clarification to address major operating subdivisions.</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		<p>1301.a.5.iv The 24 hours rule for change.termination of access may be too short - inconsistent with other limits in 1300. Should only apply to dismissals for cause - routine transfers should allow 3-5 days(even NRC allows 7 days for a favorable termination, and FERC allows 7 days regarding market access.)</p> <p>1301.a.6 Move to 1306</p> <p>1301.d.1 on-site reviews every three years What does this mean? Period is acceptable if review is part of a NERC audit, but too frequent if conducted by a hired auditor.</p> <p>1301.d.2 (and throughout the document) make the reference three calendar years for clarity and consistency in the reference for retention of audit records.</p> <p>1301.d.3.ii, change from address and phone number to business contact information. Also on page 5, 1301.b.5.iii to ensure the protection of the identity/personal information of the affected individuals</p> <p>1301.d.3.iv, request clarification that this audit applies to only audits on RS 1300, carried out by the compliance monitor</p> <p>Recommend that under Regional Differences, it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on 30 days of the deviation. Also please explain the difference between deviation and exception. This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>An authorizing authority has been designated but a formal process does not exist to</p> <p>test, validate and deploy systems into production, or (CHGE believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept,</p>	<p>been designated but a formal process to validate and promote systems to production does not exist"</p> <p>1301.5.4.11 removed</p>

Name	Company	Comments	Drafting Team Response
		<p>change Executive Management to Senior Management for consistency and clarity.</p>	
		<p>1301.e.4.xi, repeat of the earlier 24 hours if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p>	
		<p>CHGE Participating Members believe that the concept of the Bulk Electric System and association definitions may not be appropriate to capture the intent of the standard. CHGE suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Ray Morella	First Energy	<p>1301 Security Management Controls Section</p> <p>Page 3: Several sections of 1301 will require coordination at executive level across business units throughout corporations. These types of sweeping administrative documentation requirements will prove extremely time consuming and, therefore, expensive to implement under the proposed 1300 language. Some are already inherent in the organization charts, operating procedures, and job descriptions of the corporation. Standard 1300, as proposed, will simply create redundant corporate documentation in these cases because (while documentation may exist) it may not be in a format readily available for Standard 1300 audit review. If no relevant threat information exists or the costs and benefits do not warrant implementation, ABC recommends section such as those listed below be eliminated or modified.</p> <p>Governance section, which requires entities to document structure for decision making at executive level.</p> <ul style="list-style-type: none"> <li>o The Cyber Security Policy section of 1301 requires that senior management acknowledge responsibility for cyber security. Therefore the 'decision making' at the executive level is covered in the Policy section, making the governance section un-necessary.</li> </ul> <p>Roles &amp; Responsibilities requiring participants to "maintain in its policy the defined roles &amp; responsibilities..."</p> <ul style="list-style-type: none"> <li>o If The Roles &amp; Responsibilities section is not deleted entirely, then at least delete the second paragraph: 'The responsible entity shall also define the roles and responsibilities of critical cyber asset owners, custodians, and users...identified and classified in section 1.2'. From the existing numbering system used, it is not clear what "1.2" refers to.</li> </ul> <p>Page 4: "Authorization to Place into Production," part of Section 1301, requires entities to "identify the controls for testing...and document that a system has passed testing criteria." ABC agrees that a testing procedure is required. However 1301 language as proposed requires redundant documentation over and above requirements as spelled out on p. 26 and 28 in the "Test Procedures" part of Section 1306. Section 1306, "Test Procedures" (p. 28) states "...change control documentation shall include records of test procedures, results of acceptance of successful completion...documentation shall verify that all changes to critical cyber assets were successfully tested...prior to being rolled into production..." Recommendation: Section 1301 authorization to Place into Production section (for the most part) is redundant to Section 1306 Test Procedures. If the following sentence was added to Section 1306, Test Procedures, then all of "Authorization to Place into Production" section could be eliminated. "Responsible entities shall designate</p>	<p>The requirements of 1301 do not require a specific format of documentation only that the entity does document its processes. Most auditors will review your documentation to determine how it lines up with the requirements. Many of these requirements are expanded from 1200 and therefore should not introduce significant additional strain on organizations.</p> <p>1301 Security Management Controls requires a control structure to monitor and ensure compliance with this standard. As such, Governance does not reside with one person. Rather, Governance is part of the corporate culture.</p> <p>1.2 has been renumbered to read 1301.1.2</p> <p>Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>The FAQ was provided as the drafting team's explanation of some of the sections. It is not part of the standard and will not be incorporated into it. It is merely an aid.</p> <p>Access Revocation/Changes section has been re-worded to be more consistent throughout the document.</p> <p>The drafting team disagrees with removing the term "all information" primarily because it is up to each entity to determine what information relates to critical cyber assets.</p> <p>A minimum level of protection would be the minimum amount of processes and procedures in place to meet requirements and ensure that the entities critical cyber assets are reasonably protected from loss or compromise.</p> <p>Drafting team disagrees with limiting levels of noncompliance on level 4. Level 4 indicates that a company has done little to even begin to comply with the standard. However, these are not cumulative. Not having one of the requirements complete will not necessarily trigger a noncompliance.</p> <p>Access changes not being accomplished within 24 hours has been eliminated.</p>



Name	Company	Comments	Drafting Team Response
		<p>approving authority that will formally authorize that a system has passed testing criteria." Appropriate references to associated non-compliance items would also have to be eliminated.</p> <p>NERC's recently published FAQ's on Standard 1300 actually adds additional issues. Standard 1300 calls for "...entities to...identify controls...designate approving authorities that will formally authorize and document that a system has passed testing criteria....approving authority shall be responsible for verifying that a system meet minimum security configurations standards." There is nothing in the Standard 1300 which states the approving party cannot be an operator, programmer, or owner of the system. Yet in the FAQ for Standard 1300, NERC states " ...assign accountability to someone other than the operator, programmer, or owner of the systems to ensure that ..." testing has been completed. It appears that NERC is adding yet more requirements, ie., (separation of duties,) through the use of FAQ posting. ABC recommends that if requirements are not spelled out in the Standard language, additional requirements (such as this type of separation of duties) should not be introduced via the FAQ publications.</p> <p>Page 4: Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>Further on the subject of Access requirements, commentators stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website</p>	

Name	Company	Comments	Drafting Team Response
		<p>provided the following:</p> <p>"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence...."</p> <p>While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard.'" Since objections have not been addressed, NERC still needs to do this.</p> <p>Regarding requirements for updating access records, ABC recommends:</p> <p>(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <p>(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.</p> <p>(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.</p> <p>Page 3: (a) (2) (i) "The responsible entity shall identify "all" information, regardless of media type, related to critical cyber assets." It is impossible to certify that ALL information is identified and protected. ABC recommends that the word "all" should be deleted and language changed to: "The responsible entity shall identify information related to critical cyber assets."</p> <p>Page 3: ABC seeks guidance from NERC regarding the minimum levels of 'protection' to be afforded this information.</p> <p>Page 7: Levels of non-compliance, particularly for Level four are excessive. There are eleven (11) different items identified that can</p>	

Name	Company	Comments	Drafting Team Response
		<p>trigger a non-compliance item. This is far too many non-compliance triggers, and too burdensome. Recommendation: If the sections on Governance and Roles &amp; Responsibilities are omitted as suggested above, then these items will also be omitted from Levels of Non-compliance, making the document manageable: Level 2 delete (iii); Level 3 delete (iv); Level 4 delete (iv), (v), (vi), (viii). If Governance and Roles &amp; Responsibilities sections remain part of the document, then NERC should select 2 to 4 items from the list of 11 Level 4 triggers that will provide an indication of compliance and delete the remainder.</p> <p>Page 7 (4) (xi) The item which seeks a violation if one access change is not accomplished within 24 hours needs to be either eliminated or else modified to reflect the above recommendation that a violation is only warranted if the access is not suspended in 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems.</p>	

Name	Company	Comments	Drafting Team Response
Richard Engelbrecht	Rochester Gas & Electric	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p>	

Name	Company	Comments	Drafting Team Response
Richard Kafka	PEPCO	<p>Definition: The standard refers to a Compliance Monitor (e.g. Section 1301.d.1) but provides no additional detail. Can this be a company's internal auditors? Must it be an outside party? Recommend adding Compliance Monitor to the definitions.</p> <p>Section 1301.a.3: This section states the responsible entity shall assign a member of senior management in order to ensure compliance with the standard. Does this mean there should be only one responsible/accountable member of senior management? Most large utilities have major operating subdivisions (e.g. regulated T&amp;D, unregulated Generation, and Corporate IT)? Does one individual have to be designated or can this be a shared designation/responsibility? Section 1301.a.5.iv (Page 4): Recommend having different requirements for revocation/changes for users terminated/dismissed with cause (i.e. potential hostile employee or contractor) versus other more routine user changes (e.g. employee changing positions). Timeline for terminated/dismissed with cause should be more stringent. (Section 1306.b.2 of the draft standard does in fact make this distinction and appears to be in conflict with Section 1301.a.5.iv.) There are inconsistencies with other standards or guidelines on the timeliness needed to make the change (e.g. FERC Code of Conduct: 7 days regarding market access, NRC: 3 business days for normal changes; and inconsistencies within the draft 1300 Standard (e.g. 1306.b.2)).</p> <p>While EMS/SCADA systems and network devices may be able to meet a more stringent time criteria, this may be not be possible to meet for dial-up substation equipment.</p> <p>Each in-scope dial-up substation device would need to be manually called up and/or visited to change access passwords. This is not practical within a 24 hour period. In addition the password change would need to be communicated to all potential support staff in the same period. The effort involved will be dependent on the clarity on what is in scope for the electronic perimeter for dial-up devices that are serially connected. If the perimeter includes the serial devices the challenge will be even greater. The security risk for dial-up devices should be less than devices using routable protocol (i.e. on a network). Can and/or should dial-up have a less stringent timeline than devices using routable protocol or EMS/SCADA systems?</p> <p>Section 1301.a.6: Recommend moving to Section 1306.</p> <p>Section 1301.d.1: This section states outside reviews should be done every three years. What does this mean? Period is acceptable if review is part of NERC audit -- too frequent if conducted by hired independent auditor. Suggest longer cycle times between certification and external</p>	<p>The compliance monitor would be the entity which you certified to for the 1200 standard. The compliance monitor could be NERC, the regional authority or both. Typically, it is the regional authority that takes on the role of compliance monitor for the entities within its region.</p> <p>1301.a.3 - The standard calls for one member of senior management to be assigned to lead and be accountable for this program. That doesn't mean that this person can't delegate responsibility. The senior manager designated to ensure compliance with this standard is the one who signs off on the yearly self certification. They can have groups within the organization sub-certify to them on their compliance with the standard.</p> <p>1301.a.5.iv - Section rewritten to address business requirements of timeframes.</p> <p>1301.a.6 - Authorization to Place into Production has been moved under 1301.1.4 Governance</p> <p>1301.d.1 - This section states that the compliance monitor can schedule an on-site review. The compliance monitor is not an outside organization such as KPMG or Price-Waterhouse-Coopers.</p>

**Name**

**Company**

**Comments**

**Drafting Team Response**

reviews.



Name	Company	Comments	Drafting Team Response
Richard Kafka	PEPCO	Definition: The definition of Responsible Entity needs clarification (e.g. Is all generation included? Excluded?). Section 1301.a.3 (Page 3) uses Responsible Entity and the present definition does not assist in understanding this section.	Definition of a responsible entity is provided in the definitions sections at the beginning of the document.

Name	Company	Comments	Drafting Team Response
Robert Pelligrini	United Illuminating	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p> <p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a</p>	

Name	Company	Comments	Drafting Team Response
		<p>reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a) Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>• monitoring and control</li> <li>• load and frequency control</li> <li>• emergency actions</li> <li>• contingency analysis</li> <li>• arming of special protection systems</li> <li>• power plant control</li> <li>• substation control</li> <li>• real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p>	

Name	Company	Comments	Drafting Team Response
		<p>A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D) Known risks associated with particular technologies</p>	

Name	Company	Comments	Drafting Team Response
Robert Snow		<p data-bbox="499 175 842 207">In the Roles and Responsibilities:</p> <p data-bbox="499 232 1234 347">Senior Management of the respective entity must be responsible for providing sufficient resources (people and funding) to achieve the identified program and to provide additional resources to remedy any incidents or vulnerabilities that are identified.</p>	<p data-bbox="1234 175 1877 347">Drafting team agrees. It would be up to the individual entity to provide the appropriate level of resources to meet the conditions of this standard. How each entity goes about this is up to that individual entity and is not the responsibility of this standard to require a specific level of funding or resources to meet this standard.</p>

Name	Company	Comments	Drafting Team Response
Robert Strauss	NYSEG	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>



Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p> <p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a</p>	

Name	Company	Comments	Drafting Team Response
		<p>reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a) Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>• monitoring and control</li> <li>• load and frequency control</li> <li>• emergency actions</li> <li>• contingency analysis</li> <li>• arming of special protection systems</li> <li>• power plant control</li> <li>• substation control</li> <li>• real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p>	

Name	Company	Comments	Drafting Team Response
		<p>A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D) Known risks associated with particular technologies</p>	

Name	Company	Comments	Drafting Team Response
Roman Carter	Southern Company	<p>1301 (Security Management Controls)</p> <ul style="list-style-type: none"> <li>• There needs to be a lower limit and some grace period (at least 5 working days)for the senior management official. • (a)(5)(iii) Access reviews should be done at a minimum annually.</li> <li>• (b)(5)(ii) The list of designated personnel should be reviewed at a minimum annually as opposed to once per quarter.</li> <li>• (b)(5)(v) Change to - User access rights should be reviewed at a minimum annually.</li> <li>• (e)(2)(ii) Change to - Access to critical cyber information is not assessed in the last year.</li> </ul>	<p>Drafting team does not understand where you are referring to with the statement "There needs to be a lower limit and some grace period (at least 5 working days)for the senior management official."</p> <p>1301.a.5.iii - See Measures section</p> <p>1301.b.5.ii - Changed</p> <p>1301.b.5.v - Changed</p> <p>1301.e.2.ii - Changed</p>

Name	Company	Comments	Drafting Team Response
S. Kennedy Fell	NYISO	<p>Request clarification on what "information" is protected in 1301.a.2.</p> <p>Change 1301.a.2 from;</p> <p>"The responsible entity shall document and implement a process for the protection of information pertaining to or used by critical cyber assets."</p> <p>to</p> <p>"The responsible entity shall document and implement a process for the protection of critical information pertaining to or used by critical cyber assets." (NPCC's participating members feel that there may be some information pertaining to or used by cyber critical assets that may not be critical such as data transmittal from Dynamic Swing Recorders that may be used to analyze a disturbance.)</p> <p>Change 1301.a.2.i from;</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. At a minimum, this must include access to procedures, critical asset inventories, maps, floor plans, equipment layouts, configurations, and any related security information."</p> <p>to</p> <p>"The responsible entity shall identify all information, regardless of media type, related to critical cyber assets. This includes access to procedures, critical asset inventories, critical cyber network asset topology or similar diagrams, floor plans of computing centers, equipment layouts, configurations, disaster recovery plans, incident response plans, and any related security information. These documents should be protected as well." (NPCC's participating members have clarified what should be the intent of the language. Maps for instance, does not refer to BES electric system maps but network topology type maps.)</p> <p>Change 1301.a.3 from;</p> <p>"....entity's implementation of..."</p> <p>to</p> <p>"...entity's implementation and adherence of..."(NPCC's participating members believe it is important to stress that not only is it important to</p>	<p>The "information" is that which is associated with an entities critical cyber assets which, if compromised, would create a significant risk to the reliability and availability of the bulk electric system that the entity is responsible for.</p> <p>1301.1.2 Removed "pertaining to or used by" and replaced with "associated with".</p> <p>1301.1.2.1 Drafting team agrees. Wording changed.</p> <p>Designating a member of Senior management to be responsible for the cyber security program and getting Executive management engaged in the program are to different things and are not redundant.</p> <p>A "deviation" is where you do not fully meet a requirement of the standard but you meet some portion of it. An "exception" is where do not meet a requirement of the standard at all. An example of this would be that you did not have a person designated to lead the cyber security program for more than 30 days because the person who was in charge resigned and you are in the process of interviewing for their replacement. This would constitute a exception from the standard. Documenting the reason for the exception and the timeframe in which you expect the exception to be resolved would help to avoid a non-compliance.</p> <p>1301.1.3 Drafting team agrees. Wording changed.</p> <p>1301.1.5.4 Wording changed to eliminate specific timeframe.</p> <p>1301.2.5.1 Specific timeframes removed.</p> <p>1301.4.3.4 Word "Audit" removed and replaced with "Documented review results".</p> <p>1301.4.3.2 - changed</p> <p>The standard does not address who the Compliance Monitor should be. That is up to the regions and individual entities to decide. If we created a standard that had specific regional differences, then we would include the differences under the "Regional Differences" section.</p> <p>1301.5.2.3 Changed wording to "An authorizing authority has</p>

Name	Company	Comments	Drafting Team Response
		implement this Standard but to adhere to it as well.	been designated but a formal process to validate and promote systems to production does not exist"
		The "24 hours" in 1301.a.5.iv should be a measure. It should be a corresponding measure under 1301.b.5.	1301.5.4.11 removed
		Change 1301.a.5.iv from;	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours of a change in user access status. All access revocations/changes must be authorized and documented."	
		to	
		"Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished within 24 hours if a user is terminated for cause or for disciplinary action, or within seven calendar days for all other users of a change in user access status. All access revocations/changes must be authorized and documented." (The intent of this section was to address the situation of when an authorized user is terminated and the urgent nature of needing to respond to this.)	
		change 1301.b.5.i from;	
		"5 days"	
		to	
		"7 calendar days" (NPCC's participating members believe that the 5 days may be not be sufficient time especially when considering holiday seasons)	
		1301.d.2 (and throughout the document) make the reference "three calendar years" for clarity and consistency in the reference for retention of audit records.	
		1301.d.3.iv, request clarification that this "audit" applies to only audits on RS 1300, carried out by the compliance monitor	
		1301.d.3.ii, change from "address and phone number" to "business contact information". Also on page 5, 1301.b.5.iii to ensure the	

Name	Company	Comments	Drafting Team Response
		<p>protection of the identity/personal information of the affected individuals</p> <p>Recommend that under "Regional Differences", it be noted that each Region may have a different Compliance process therefore each Region is responsible for designating the Compliance Monitor</p> <p>1301.e.1.iii, request clarification on "30 days of the deviation". Also please explain the difference between "deviation" and "exception". This does not match the FAQ 1301 Question 4.</p> <p>1301.e.2.iii, change from;</p> <p>"An authorizing authority has been designated but a formal process to validate and promote systems to production does not exist, or "</p> <p>to</p> <p>"An authorizing authority has been designated but a formal process does not exist to test, validate and deploy systems into production, or" (NPCC believes it was the drafting team's intent to deploy the system rather than promote which has a different connotation associated with it,)</p> <p>Remove 1301.e.4.v, it is implied and redundant with 1301.e.4.i, if kept, change "Executive Management" to "Senior Management" for consistency and clarity.</p> <p>1301.e.4.xi, repeat of the earlier "24 hours" if a user is terminated for cause or for disciplinary actions, or within 7 calendar days (should be consistent with the language used in FERC ORDER 2004b-Standards of Conduct).</p> <p>NPCC Participating Members believe that the concept of the Bulk Electric System and association "definitions" may not be appropriate to capture the intent of the standard. NPCC suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p> <p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a</p>	



Name	Company	Comments	Drafting Team Response
		<p>reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a) Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>• monitoring and control</li> <li>• load and frequency control</li> <li>• emergency actions</li> <li>• contingency analysis</li> <li>• arming of special protection systems</li> <li>• power plant control</li> <li>• substation control</li> <li>• real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p>	

Name	Company	Comments	Drafting Team Response
		<p>A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D) Known risks associated with particular technologies</p>	

Name	Company	Comments	Drafting Team Response
Scott McCoy	Xcel Energy	<p>Under 1301 (a) (3), the sentence that says "This person must authorize any deviation or exception from the requirements of this standard." should be changed to read "The person that must authorize any deviation or exception from the requirements of this standard must be specified in the responsible entity's governance documentation."</p> <p>Under 1301 (d) (3) (ii), remove the word "and" at the end of the sentence.</p> <p>Under 1301 (e) (1). What is the difference between (iv) and (v)?</p>	<p>1301(a)(3) - Drafting team disagrees. The standard already requires that the person responsible for the cyber security program be documented by listing the person's name, etc. Listed under section 1301.2.3.2. Also, provision has been added to allow for the senior manager to authorize a delegate to review and authorize deviations or exceptions.</p> <p>1301.4.3.2 Accepted</p> <p>130.1.5.1.4 and .5 - No difference. 1301.5.1.5 removed.</p>

Name	Company	Comments	Drafting Team Response
Seiki Harada	BC Hydro	3) Regarding 1301 (a) (5) (iii), consider adding the condition to review access rights/privileges at least once a year.	This is required in the Measures section 1301.2.5.3

Name	Company	Comments	Drafting Team Response
Stacy Bresler	Pacificorp	<p>1301.a.2.i "...identify all information..." should be qualified as follows: "...identify all information that is owned and controlled by the entity..."</p> <p>1301.a.2.i "...shall identify..." is ambiguous terminology. Specifically, how should this information be identified? Within a spreadsheet (detached)? By means of a physical label (attached)? Both? Please clarify what is acceptable and unacceptable forms of identification.</p>	<p>1301.a.2.i - Reworded to say "The responsible entity shall identify all information, regardless of media type, related to the entities critical cyber assets."</p> <p>How you "identify" this information is up to you. It should be clear enough that any user would be able to determine the information's level of sensitivity regardless of the type of media the information resides on. The Drafting team suggests that you investigate some of the government rules on identification and classification of information as a guideline.</p>

Name	Company	Comments	Drafting Team Response
Terry Doern	BPA	<p>Is "cyber assets affecting" the same as "critical cyber assets"?</p> <p>1301.a.2 BPA is bound by DOE Order 457.3 in how it protects information that is categorized as OUO (Official Use Only) and CII (Critical Infrastructure Information)</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: Change Information Protection to Information Protection Program to be aligned with the references within the measurement section. 1301.a.2.i This is very, very broad. Example, "equipment layouts" could include every document related to substation equipment in the field.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment:</p> <p>Remove "all", minimum requirements is defined</p> <p>1301.a.2.ii Change the term "classify" to "categorize". As a federal agency the term "classify" has a different meaning than what is implied here (e.g., classify = TOP SECRET). This comment applies to all sections herein that use the term "classified" or "classify." See NIST cyber standards.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: The use of unauthenticated personnel is anomalous to the rest of the document. Unauthorized is a better term. Even some authenticated personnel may not necessarily be authorized.</p> <p>1301.a.2.iiiBPA Transmission is in agreement with the WECC EMS WG's comment: "as defined by the individual entity" should be included after classification level to read "...classification level as defined by the individual entity." It would even be better to use standard language here. FIPS 199 give a method of defining security levels which may be more appropriate</p> <p>The phrase "identify the information access limitations" is unclear. Change to "prescribe protection measures based on categorization for critical cyber asset information."</p> <p>1301.a.3 Separate the assignment of roles from the definition of roles. 1301.a.5.1The term "access management to information" is unclear.</p>	<p>Yes</p> <p>1301.a.2 - DOE requirements would supecede NERC requirements. Where they conflict, the DOE requirements would take precedence and an exception to the NERC standard could be written to document the disparity.</p> <p>Drafting team disagrees - The section title "Information Protection" is identical to the one in the measurements section. Information Protection is used as a section heading to denote a program and controls for the protection of information.</p> <p>1301.a.2.1 - This applies only to identified critical cyber assets. Each entity will need to identify what it believes to be critical cyber asset information. The section has been rewored to provide more clarity.</p> <p>1301.a.2.i - Drafting team disagrees with removing the word "all". The statement following provides examples of types of information to include but is not and all inclusive or minimum requirements list.</p> <p>1301.a.2.ii - Changed</p> <p>"Unauthenticated" changed to "unauthorized"</p> <p>1301.a.2.iii - Changed</p> <p>"identify the information access limitations" changed to "identify the information access controls"</p> <p>1301.a.3 - Drafting team disagrees. Both statements fall under the section heading of "Roles and Responsibilities". Breaking them out into subsections add no real value to the standard.</p> <p>1301.a.5.1 - Section has been rewored.</p> <p>1301.a.5.iv - Section has been rewored.</p> <p>1301.b.1.ii - Drafting team disagrees. Does not add clarity. This measure addresses the issue of the entity maintianing its written cyber security policy where the entity's commitment to protect critical cyber assets is stated. The team believes that this statement would not necessarily be repeated in all policy documents.</p>

Name	Company	Comments	Drafting Team Response
		<p>BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "or used by".</p> <p>1301.a.5.iv Access Revocation/Changes: Should be reworded to read: Responsible entities shall define procedures to ensure that modification, suspension, and termination of user access to critical cyber assets is accomplished in a time frame that ensures critical cyber assets are not compromised.</p> <p>1301.b.1.ii Change "its written cyber security policy" to "a written cyber security policy(s)." This comment applies to all sections herein that use "its policy".</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: Policies are supposed to be broad with a life cycle of 3-5 years. This should be changed to "reviewed as needed with a minimum review of every 5 years".</p> <p>1301.b.2 Define Information Protection and Cyber Security. BPA treats these as one program.</p> <p>In the phrase "to the classification level assigned to that information.", change "classification" to "sensitivity".</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: To be consistent, change title to Information Protection Program.</p> <p>1301.b.5.i BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "within five days" from section (i). The effort required to make this an auditable function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>1301.b.5.ii The review periods seem to be too often and don't seem to synchronize with each other in this section.</p> <p>1301.b.6 In federal terms this is the Accreditation portion of a certification and accreditation process. I don't see any mention of an Interim Authority to operate, which recognizes significant risks, and accepts them for a given period of time, while providing (within the organization) a corrective action for those risks.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: Remove the last line. The effort required to make this an auditable</p>	<p>Life cycle review changed to read "not to exceed 3 years."</p> <p>1301.b.2 - The sections you refer to talk about measures for the Cyber Security Policy and Information Protection Program. While an information protection program can be part of a Cyber Security Policy, the drafting team feels that the two terms are not identical in their scope.</p> <p>1301.b.2.iii - Reworded "classification level" to "categorization level"</p> <p>1301.b.5.i - Timeframe modified to be more in keeping with business needs.</p> <p>1301.b.5.ii - Timeframe changed to annually.</p> <p>1301.b.6 - Section reworded and moved under governance.</p> <p>1301.d.1 - Drafting team disagrees. The term "investigation" does not always imply criminal activity. Most entities within NERC are part of private industry and not federal entities. While the drafting team understands BPA's viewpoints, the standard is written more towards a private sector audience.</p> <p>1301.d.2 - The audit by the compliance monitor is conducted according to NERC guidelines.</p> <p>1301.d.3 - Drafting team disagrees. The written cyber security policy is defined in the scope of this standard. If BPA feels the need to enter into a non-disclosure agreement with the compliance monitor, the drafting team feels that those particular requirements of federal organizations can be addressed and dealt with on an individual basis.</p>

Name	Company	Comments	Drafting Team Response
		<p>function only creates unnecessary administrative overhead and distracts from the intent of the control.</p> <p>1301.d.1 Change "investigations" to "inquiry". In Federal perspective investigation means criminal. Clarify who can file Complaints.</p> <p>1301.d.2 Refer to Audit records section.</p> <p>1301.d.3 "Written cyber security policy" needs to be redefined as "Any written cyber security policy(s) which incorporates the requirements of this standard." As a federal agency, public entities such as NERC compliance monitors may not have access to all BPA's policies or procedures under applicable regulation or law. There is no provision here for non-disclosure agreements with the compliance monitor. This will limit the scope to what others has access to.</p>	



Name	Company	Comments	Drafting Team Response
Tom Flowers	Centerpoint Energy	<p>Page 3, 1301 Security Management Controls</p> <p>General comment:</p> <p>This section uses the term "responsible entities" while most other sections use "the responsible entity". Choose one and be consistent.</p> <p>Specific Comments:</p> <p>Page 3, Introduction</p> <p>Insert this as the third sentence. "Each entity will have to modify or adjust the requirements below to deal with environmental, technical, logistic, personnel, and access differences between attended facilities such as Control Centers and Power Plants and critical Substations which are typically unattended."</p> <p>Page 3, (a)(1) Requirements -- Cyber Security Policy</p> <p>Replace the paragraph with..."The responsible entity shall create and maintain a role based Cyber security policy that addresses the requirements of this standard as well as the unique roles and responsibilities at each entity. "</p> <p>Page 3, (a)(3) Roles and Responsibilities</p> <p>Replace "member" with..."member(s) "</p> <p>Replace "the Cyber security standard" with... "this Cyber security standard and all related policies, procedures, and practices unique to the entity."</p> <p>Replace "person" with..."person(s) "</p> <p>Replace "section 1.2" with... "subsection (a)(2) above."</p> <p>Page 4, (a)(5)(iv) Access Revocation/Changes</p> <p>Replace the first sentence with... "The responsible entity shall define procedures to ensure that modifications, suspension, and termination of user access to critical Cyber assets are accomplished in a timely manner. Revocation/changes of access due to termination for cause or suspension shall be accomplished within 24 hours while normal termination, transfer, or change of responsibilities shall be accomplished within 5 days "</p> <p>Page 4, (a)(6) Authorization to Place into Production</p> <p>Delete this subsection. This subsection should be moved to section 1306.</p>	<p>"Responsible entities" - Drafting team disagrees. There is no gramatic difference in the usage.</p> <p>Introduction - Drafting team disagrees. Statement adds confusion to the standard. By allowing each entity to "modify or adjust" this standard at will provides no real measure of compliance with a national standard.</p> <p>1301.a.1 - Drafting team disagrees. The creation, maintainance and implementation of the cyber security policy is up to each entity to determine.</p> <p>1301.a.3 - Drafting team disagrees. One member of senior management must be the leader of the program and ultimately accountable for the program.</p> <p>Section 1.2 corrected to read 1301.1.2</p> <p>1301.a.5.iv - Section has been reworded to reflect timeframes that are more in keeping with business needs.</p> <p>Page 4, (a)(6) Authorization to Place into Production has been moved under 1301.1.4 Governance</p>

Name	Company	Comments	Drafting Team Response
Tom Pruitt	Duke Energy	<p>1301 Does this require a data "classification" system and a personnel "clearance" system to be created? Do we have to stamp/mark any potential critical info? The "Separation of Duties" referenced in FAQ#8 should be explicitly stated in the standard.</p> <p>1301(2)(i) &amp;(v), pg 4 Suggest that these reviews be at least every two years to reduce administrative costs of policy implementation.</p> <p>1301(a)(1)(ii) Please define "unauthenticated personnel."</p> <p>1301(a)(3), pg 3 Duke agrees whole-heartedly with the need for senior management leadership and management of the implementation of the NERC 1300 standard. However, the detailed tasks listed in these two sections seem to be particularly onerous and timeconsuming for a senior manager to personally conduct. We would suggest that for "authorization of any deviation or exception" and for approval of lists of assets, that these tasks be something that could be delegated by the senior manager (particularly the approval of exceptions).</p> <p>1301(a)(5)(i) &amp; 1301(a)(5)(ii) The burden of applying such controls on systems at generation and transmission stations is great. The incremental benefit of doing so, taking into account the amount of controls already in place, is minimal.</p> <p>1301(a)(5)(iii) What is the frequency of review?</p> <p>Section Comment for NERC 1301(a)(5)(iv) Evaluate changing 24 hours to 2 weeks. For example, physical access to a nuclear station is revoked within the stated 24 hours. Other than that, 24 hours is overly restrictive for revoking access to a single component or system (i.e. turbine control system). In some cases our equipment is not capable of such change. In this case, we are relying on revoking the security badge (i.e. physical access). Network accounts are also disabled within 24 hours. This prevents one from accessing through the corporate network for network connected control systems. The "within 24 hours" should only apply to terminations or required transfer. Other changes due to normal reassignments should be longer and the 10 business day period suggested by others is reasonable. For consistency, all changes to all types of access lists should be changed within 24 hours and normal work reassignments within 10 business days. Suggested re-wording: "Responsible entities shall define procedures to ensure that a modification, due to required transfers or terminations, of user access to critical cyber assets is</p>	<p>Yes, you must identify, classify and protect information related to your critical cyber assets. Without doing so, you will be unable to provide adequate protection and to educate your personnel as to what is important.</p> <p>The "Separation of Duties" reference in the FAQ is provided as an example. The FAQ will not be part of the standard.</p> <p>1301.2.1 changed to "not to exceed 3 years"; 1301.2.4 - Drafting team disagrees. Review of these relationships to ensure that any changes in the governance structure is documented and communicated keeps executive management informed and engaged.</p> <p>1301.1.1.2 - Change to "unauthorized personnel"</p> <p>1301.1.3 - It is perfectly acceptable for the senior manager to delegate someone to serve in his/her behalf for the review and authorization of exceptions/deviations providing that this delegation of responsibilities is fully documented including the level of authority the delegate will have. Added the wording "This person, or their designated delegate, must authorize any deviation"</p> <p>1301.2.6 Authorization to Place into Production has been moved under 1301.2.4 Governance</p> <p>1301.1.5.4 Access Revocation section re-worded to permit the entities to define the processes that work best for their environments and protect their critical cyber assets.</p> <p>1301.1.5.3 Added frequency of review to Measures section</p> <p>Access revocation processes will be up to each entity. Sections re-worded to reflect this.</p> <p>1301.2.2.1 Drafting team rejects the suggestion to change annual review to every 2 years. Review of the program is to ensure that it still meets the mission of the company, current business environment and compliance with this standard.</p> <p>1201.2.2.2 This section applies to the information security protection program. The drafting team does not understand what 6 other areas are being referred to.</p>

Name	Company	Comments	Drafting Team Response
		<p>accomplished within 24 hours of the change having taken place. Other modifications, due to normal transfers, of user access to critical cyber assets is accomplished within 10 business days of the change having taken place. All access revocations/changes must be authorized and documented." Consistency is needed for delegation of approval. Suggested re-wording: "The responsible entity shall maintain documentation of any deviations or exemptions authorized by the current senior management official or designee responsible for the cyber security program."</p> <p>1301(b)(2)(i) Request that these reviews be at least every two years to reduce administrative costs of policy implementation.</p> <p>1301(b)(2)(ii) This section on controls has six other areas associated with control issues and many of them also have an annual review cycle. There should be some consistency since all six areas are of importance.</p> <p>1301(b)(5)(i) Consider changing five (5) days to 2 weeks. See comment for section 1301(a)(5)(iv) above.</p> <p>1301(b)(5)(ii) Why wouldn't the entity audit this annually, like all the other items? This should be evaluated for combination with 1301(b)(4).</p> <p>1301(b)(5)(iii) This is quite a burden for a generation station with little benefit. The list would be small, and the list of systems/applications would be "all."</p> <p>1301(b)(5)(v) Quarterly is too often, but should be done at least annually. Suggested re-wording: "The responsible entity shall review user access rights periodically and at least annually to confirm access is still required."</p> <p>1301(b)(6) Authorization to place into production when? After maintenance? After modification? New devices? Define production environment? Is that "physically mounted" or "operational"? Why 48 hours? Standardize on 2 weeks. Too many frequencies (i.e. 24 hours for one thing, 48 for another, 2 weeks, quarterly, annually) is going to be very confusing and is likely to be missed. Standardize on time periods for different type of activities. Elsewhere 5 days is used to complete a change to a list identifying authorizing individuals. Suggested rewording: "Changes to the designated approving authority shall be documented within 5 business days of the effective change. If a person's title, phone or address changes mid-year, is this required to be documented within 48 hours of the change?"</p> <p>1301(d)(2) Please define performance-reset period.</p>	<p>1301.2.5.1 Changed</p> <p>1301.2.5.2 Added annual audit measure</p> <p>1301.2.5.3 The drafting team maintains that the list of authorizers and systems/applications needs to be maintained regardless of the size of the list. The standard cannot differentiate between the sizes or staffing of entities' facilities.</p> <p>1301.2.5.5 removed</p> <p>1301.2..6 Authorization to place into production is a management control to be defined by the entity. As such, it has been moved under Governance.</p> <p>1301.4.2 Performance reset period is a compliance issue that will be addressed separately.</p> <p>1301(iv), pg 5 This section has been re-worded to allow each entity to define access revocation periods that are appropriate with business processes and yet protect the entities critical cyber assets.</p>

Name	Company	Comments	Drafting Team Response
		1301(iv), pg 5 Request that this time period be extended to 10 business days for current employees with status change that no longer requires access to critical cyber assets, 1 business day for terminated employees.	

## Section 1302 Comments and Drafting Team Responses

Name	Company	Comments	Drafting Team Responses
A. Ralph Rufrano	NYPA	<p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose</p>

Name	Company	Comments	Drafting Team Responses
		<p>on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets</p> <p>(i) The responsible entity shall maintain its critical bulk electric system</p>	<p>a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Previous section 1302.g has been re-drafted as suggested.</p>

Name	Company	Comments	Drafting Team Responses
		assets approved list as identified in 1302.1.1."	
		to	
		"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."	
		Change 1302.g.2.i from;	
		"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."	
		to	
		"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).	
		Change 1302.g.5 from;	
		"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"	
		to	
		"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to	

Name	Company	Comments	Drafting Team Responses
		<p>assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302;</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	



Name	Company	Comments	Drafting Team Responses
Allen Berman	LIPA	<p>1302 Critical Cyber Assets</p> <p>General Comments: Lettering of bullets must be corrected. Remove sub-bullets for sections with single requirements.</p> <p>Regarding the identification, documentation and use of Critical Bulk Electric System Assets to identify Critical Cyber Assets</p> <p>Entities adhering to this standard should have the responsibility and flexibility of identifying critical cyber assets without tracking the critical bulk electric system assets. If the intention of the standard is to strengthen cyber security, the focus should be guided in that direction.</p> <p>Introduction Comment: Suggest changing the last sentence to read "This standard requires that entities identify and protect critical cyber assets that support the reliable operation of the bulk electric system."</p> <p>(a)Requirements (2) Critical Cyber Assets Comment: Isn't this description different than what's presented in the "Definitions" section of the document? If so, why?</p> <p>(i)Compliance Monitoring Process (2) Comment: Are we to understand from this bullet that we will be audited annually to confirm compliance? Why is data kept for three calendar years, but audit records for three years? The use of the word "calendar" in some time-based requirements and not in others may lead to confusion. Was this intentional? Otherwise, please correct for consistency.</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Entities adhering to this standard will have the responsibility to identify and track critical cyber assets and the associated critical assets. All bulk electric system assets do not need to be tracked.</p> <p>The definition of Critical Cyber Assets has been removed. Critical Cyber Assets are to be determined as per the revised section 1302.</p> <p>With regards to 1302.4, Compliance Monitoring, the section has been modified to be clearer with regards to what must actions must occur on what cycle – i.e.; 30 days, six months, one calendar year, three calendar years. It is also re-drafted to be clearer has to what data must be retained, and for how long.</p>

Name	Company	Comments	Drafting Team Responses
Charles Yeung	SPP	<p>1302 (a) (1) Critical Bulk Electric System Assets: The definition needs to quantify the subjective term "large quantities of customers" either as MW load served or percentage of customers served. "Large quantites" is too vague. The definition needs to quantify the term "extended period of time." Is this hours? Days? Weeks?</p> <p>1302 (a) (1) (i) Critical Bulk Electric System Assets: Presumed incorrectly placed comma, alters meaning. Should the requirement read ". . . such as telemetry, monitoring and control, . . ." or ". . .such as telemetry monitoring and control, . . ."?</p>	<p>Such phrases as "large quantities of customers" and "extended period of time" have been removed.</p> <p>"Telemetry" and "monitoring and Control" were written as intended with "telemetry" being without remote control capabilities.</p>
Charlie Salamone	NSTAR	<p>1302.a.1.i.A - Define Telemetry</p> <p>1302.a.2.i - Items B and C should be sub-bullets of requirement 1302.a</p>	<p>Telemetry changed to telemetry which is a term defined in the NERC Version 0 glossary.</p> <p>Sub-bullets corrected in 1302.a.2.i</p>

Name	Company	Comments	Drafting Team Responses
Chris DeGaffenried	NYPA	<p>1302 Critical Cyber Assets</p> <p>Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a) Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>* monitoring and control</li> <li>* load and frequency control</li> <li>* emergency actions</li> </ul>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<ul style="list-style-type: none"> <li>* contingency analysis</li> <li>* arming of special protection systems</li> <li>* power plant control</li> <li>* substation control</li> <li>* real-time information exchange</li> </ul>	essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.
		(2) Critical Cyber Assets	In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.
		(i) In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:	We have also declined to provide other references to items such as “high-jacking” or “day zero attacks.” While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.
		A) The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.	
		B) The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.	Previous section 1302.g has been re-drafted as suggested.
		C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.	
		D) Known risks associated with particular technologies	
		Change 1302.g.1 from;	
		"1 Critical Bulk Electric System Assets	
		(i) The responsible entity shall maintain its critical bulk electric system	
		assets approved list as identified in 1302.1.1."	
		to	
		"1 Critical Bulk Electric System Operating Functions and Tasks	
		(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in	

Name	Company	Comments	Drafting Team Responses
		1302.a.1."	
		Change 1302.g.2.i from;	
		"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."	
		to	
		"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).	
		Change 1302.g.5 from;	
		"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"	
		to	
		"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)	
		Change 1302.g.5.i from;	
		"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."	

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302; "critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	
Dave Magnuson	Puget Sound Energy	<p>1302 Critical Cyber Assets (a) ( 1) (i) (A)Does protection include telecom paths even though "telemetry" not included? (e.g, RAS schemes linked by telecom)</p> <p>1302 Critical Cyber Assets (a) (1) (vi) Add reference to RAS schemes used on West Coast. "Special Protection Systems" = an east coast term.</p>	<p>Telecom paths are not included. The system(s) sitting at one or both ends are. This acknowledges the fact that often the telecom paths are not 100% controllable by responsible entities.</p> <p>Special Protection System (SPS) is defined in the NERC Version 0 glossary of terms, while Remedial Action Scheme (RAS) reference in the glossary simply refers to the SPS definition. Therefore, RAS is not mentioned in the Nerc Cyber Security Standard.</p>

Name	Company	Comments	Drafting Team Responses
Dave McCoy	Great Plains Energy	<p>1302 -- Should the risk assessment consider collections of bulk electric system assets, all supported by the same cyber asset, which taken collectively could, by their destruction or compromise, have a significant impact on the ability to serve large quantities of customers for an extended period of time or would have a detrimental impact on the reliability or operability of the electric grid or would cause significant risk to public health and safety? Or is it allowable for the risk assessment to consider only single bulk electric system assets 1302 - Under Requirements under Critical Cyber Assets the first criteria is for cyber assets that support a critical bulk electric system asset. Some clarification of the word support would be helpful. Does support include control, configuration, monitoring or historic reporting? This should be clarified, because there are accounting-type systems and asset management systems that support critical assets, but would not be typically be considered critical since compromising such systems will not result in loss of load or system reliability. For example, would distribution capacitor control, transmission line monitoring or asset management/transformer maintenance prediction systems be considered critical cyber assets?</p> <p>1302 - Under Requirements under Critical Bulk Electric System Assets there is a list of examples of critical assets, but it would be helpful if you could be more specific. For example, would it be fair to say that critical bulk electric system assets are limited to those assets that if compromised could cause an outage of 300MW or more for 15 seconds or longer? Such a definition would provide the industry with a consistent yardstick for determining critical assets.</p>	<p>If the loss or compromise of a single cyber asset can have a significant negative impact on multiple BES assets, functions, or tasks, then the collective attribute must be assets for criticality.</p> <p>The use of terms like "control" and "support" imply that if the loss or compromise of the cyber asset has significant negative impact on maintaining reliable operation of the BES, and is accessible via a routable protocol or dial-up, then it is a critical cyber asset.</p> <p>While 1300 provides some criteria for assessing whether a BES asset, function, or task might be critical, it is not within the scope of this standard to further establish a standard for critical BES assets, functions, or tasks. Additionally, terms such as you suggested might not be considered critical in other regions or control arears.</p> <p>Allowable outage times for critical assets or critical assets are not speciiied in 1300 as cyber security protection from various threats is either required or not according to the standard.</p>

Name	Company	Comments	Drafting Team Responses
Dave Norton	Entergy Transmission	<p>9. General Comment -- "Risk-Based Assessments": The standard requires use of a risk-based assessment to identify critical system assets, but needs to offer some kind of hard guidance on parameters. This is actually an offshoot of comment #8 immediately above. How many customers must be affected before an impact is significant - as either an absolute number, or percentage? How many hours is "an extended period of time". Unless and until criteria for what constitutes a significant impact is clearly proffered, risk assessment activities will be largely meaningless. The outcome of a "risk assessment" is not a list of vulnerabilities; it's a measure of financial exposure, used thereby to correctly determine how much money should be spent to effect countermeasures.</p> <p>14. Page 9, paragraph (a) - Section 1302: "Critical Cyber Assets" -- The requirements to define and document all critical assets is a concern that was raised to FERC last year. They wanted utilities to document their critical assets and allow FERC to see these. Many/most utilities refused to allow FERC to view these documents from fear that they would be required under the Freedom of Information Act to make these documents public. The same concern is raised here; what is the guarantee that these documents remain "hidden" from all eyes except the information owner?</p> <p>15. Page 9: Responsible Entity Definition -- This does not lead to being able to clearly distinguish between the requirements of a transmission owner verses, say, the requirements of a coop, or requirements incumbent upon industrial customers when they own a substation on a responsible entity's transmission system. Is the transmission systems owner responsible for non-owned cyber assets at work on the part of the bulk electric power grid for which it has oversight? That seems unreasonable. 1300 uses the concepts/terms "reliability entity" and "responsible entity" rather than "transmission system owner" and/or "transmission asset owner." It would seem that the owner of the critical cyber asset should be responsible for compliance, and that all owners of critical cyber assets attached to the grid must be subject to the same regulation. Otherwise, there will be "weak links" across and throughout the greater system.</p>	<p>9 - Agreed. Such references have been removed.</p> <p>14 - The attempt is not to define critical BES assets, functions, or tasks (aft's). It does try to provide a limited set of criteria to determine a minimum list of essential BES AFT's.</p> <p>15 - Based on the current NERC Functional Model, the 1300 SAR document clearly delineated those organizations that are "responsible entities." I could not find where in 1302 the "reliable entities" was used.</p> <p>16 - 1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose their preferred methodology for their environment.</p> <p>17 - The former section D was overly weighted due to the sequencing problems. We believe this has been corrected with re-drafting.</p>



Name	Company	Comments	Drafting Team Responses
		<p>16. Page 9 - Who Decides: RC or Asset Owner? - Continuing along the lines of discussion immediately above, who first will decide what assets are critical to the bulk electric power system. The application of cyber security measures only applies to cyber assets at work in facilities/sites deemed to be critical to the reliability of the bulk electric power grid. What if an RC and the asset owner disagree about the criticality of an asset in question -- who decides? How would disagreements be resolved?</p> <p>17. Page 10: The critical cyber asset definition is overly broad. The current definition in section D) would include all remote terminal units and microprocessor based relays that have dial-up maintenance ports. Section E) would define an IP based printer in a control center as a critical cyber asset solely because it's housed within the electronic security perimeter of a set of critical bulk electric system assets. There is no consideration of the actual operational use of the asset.</p>	

Name	Company	Comments	Drafting Team Responses
David Kiguel	Hydro One	<p>Consistent with the above, we recommend to replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below.</p> <p>"1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies."</p> <p>-----</p> <p>Change 1302.g.1 from</p> <p>"1 Critical Bulk Electric System Assets</p> <p>(i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Previous section 1302.g has been re-drafted as suggested.</p>

Name	Company	Comments	Drafting Team Responses
		<p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1." -----</p> <p>Change 1302.g.2.i from</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." -----</p> <p>Change 1302.g.5 from</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p> <p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" -----</p> <p>Change 1302.g.5.i from</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p>	

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>-----</p> <p>---</p> <p>In 1302, change</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks."</p> <p>-----</p>	

Name	Company	Comments	Drafting Team Responses
David Little	Nova Scotia Power	<p>1302</p> <p>The Critical Bulk Electric System Assets section is too prescriptive in defining the included elements. We suggest that the focus should be on function and suggests the substantive changes as shown below to address this issue with the term Critical Functions and Tasks that relate to the inter-connected transmission system.</p> <p>Replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets</p> <p>Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data.</p> <p>This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements</p> <p>Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:</p> <ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>Change 1302.g.1 from; 1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Previous section 1302.g has been re-drafted as suggested.</p>

Name	Company	Comments	Drafting Team Responses
		<p>assets approved list as identified in 1302.1.1. to 1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1.</p> <p>Change 1302.g.2.i from; The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure. to The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.</p> <p>Change 1302.g.5 from; Critical Bulk Electric System Asset and Critical Cyber Asset List Approval to Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval (it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations is lost.)</p> <p>Change 1302.g.5.i from; A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained. to A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained.</p>	



Name	Company	Comments	Drafting Team Responses
		Change 1302; critical bulk electric system assets to critical bulk electric system operating functions and tasks	

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	<p>1302 Critical Cyber Assets</p> <p>(a) Requirements Responsible entities shall identify their critical bulk electric system assets using their preferred risk-based assessment. An inventory of critical bulk electric system assets is then the basis to identify a list of associated critical cyber assets that is to be protected by this standard. Doesn't NERC provide guidance to help define critical bulk electric system assets? This would seem to be fundamental to this process. This would seem necessary in order to ensure that entities address assets at their boundaries such that their interconnection partners designate the same boundary assets. Aren't the assets to be protected by the responsible entity's cyber security policy and its attendant procedures and practices? This standard only sets the requirements for the entity's actions. It is unclear why the authors appear to be including non-cyber bulk electric system assets in this standard. In general, such critical assets would appear to be outside the scope of this standard and should be addressed in other appropriate plans and assessments, including those for continuity of operations. Once such critical asset identification is complete, and where it identifies critical cyber assets, then the protection of those cyber assets is covered by this standard. As prepared, this section is confusing.</p> <p>(ii) Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) - It is unclear how this is a critical cyber asset.</p> <p>(iii) Generation: A) Generating resources under control of a common system that meet criteria for a Reportable Disturbance (NERC Policy 1.B, Section 2.4) Perhaps this could be clearer if worded as "Cyber systems providing centralized control of generating resources meeting the criteria for a Reportable Disturbance..." It appears that what is being attempted here is the identification of Critical Cyber Assets in terms of the power system and impact, but it is being attempted in a way that appears backwards. This is common to</p>	<p>Each NERC Standard must specify any applicable "Critical Bulk Electric System Assets, Functions, and Tasks".</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with oversight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p>

Name	Company	Comments	Drafting Team Responses
		<p>other material under this subparagraph and makes the application of this standard difficult.</p> <p>B) the cyber asset uses a routable protocol, or - Although a routable protocol is significant from the perspective of a cyber system exposed to other interconnected systems, this may not be a good indicator for a critical cyber asset. A critical cyber asset should be identified based on its impact on the power system or the business functions of the responsible entity. Based upon this assessment, the risks faced by the entity (and the industry should the system be compromised) can be established. The vulnerabilities presented by the use of a particular protocol can then be examined in the context of exposure (e.g., the use of a routable protocol on an isolated minor system whose compromise would have little business impact, does not qualify it for categorization as critical.)</p> <p>C) the cyber asset is dial-up accessible. Similar comment to that above. Exposure is assumed, however. Nevertheless, the impact of the system and its compromise through the exposure mechanism must be considered before the system should be categorized as critical. In addition, mitigating controls, such as dial-up through a private branch exchange or the employment of dial-back technology must be considered.</p> <p>D) Dial-up accessible critical cyber assets, which do use a routable protocol require only an electronic security perimeter for the remote electronic access without the associated physical security perimeter.</p>	<p>Implementation of NERC cyber security is focused on BES assets which provide critical operating functions and tasks and not all BES assets.</p> <p>Non-cyber assets BES assets are included in the cyber security standard only if those non-critical cyber assets are within the same electronic security perimeter as critical cyber assets and therefore present a cyber risk to the critical cyber assets.</p> <p>Agreed, sub-stations associated with IROL are not critical cyber assets. But the cyber assets performing or supporting IROL functions and tasks might be. We believe the intent with IROL and Reporting Disturbance is clearer with the re-drafting.</p> <p>As the re-drafting will clarify, it is the role of the cyber asset first, then in conjunction with its use of a routable protocol or dial-up for access, that qualifies it for compliance. Identifying cyber assets using routable protocols again helps to focus implementation on those cyber assets with increase cyber exposure.</p>

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	<p>1302 Critical Cyber Assets</p> <p>(a) Requirements</p> <p>Responsible entities shall identify their critical bulk electric system assets using their preferred risk-based assessment. An inventory of critical bulk electric system assets is then the basis to identify a list of associated critical cyber assets that is to be protected by this standard. Doesn't NERC provide guidance to help define critical bulk electric system assets? This would seem to be fundamental to this process. This would seem necessary in order to ensure that entities address assets at their boundaries such that their interconnection partners designate the same boundary assets. Aren't the assets to be protected by the responsible entity's cyber security policy and its attendant procedures and practices? This standard only sets the requirements for the entity's actions. It is unclear why the authors appear to be including non-cyber bulk electric system assets in this standard. In general, such critical assets would appear to be outside the scope of this standard and should be addressed in other appropriate plans and assessments, including those for continuity of operations. Once such critical asset identification is complete, and where it identifies critical cyber assets, then the protection of those cyber assets is covered by this standard. As prepared, this section is confusing.</p> <p>(ii) Transmission substations associated with elements monitored as Interconnection Reliability Operating Limits (IROL) - It is unclear how this is a critical cyber asset.</p> <p>(iii) Generation:</p> <p>A) Generating resources under control of a common system that meet criteria for a Reportable Disturbance (NERC Policy 1.B, Section 2.4) Perhaps this could be clearer if worded as "Cyber systems providing centralized control of generating resources meeting the criteria for a Reportable Disturbance..." It appears that what is being attempted here is the identification of Critical Cyber Assets in terms of the power system and impact, but it is being attempted in a way that appears backwards. This is common to</p>	---- redundant ----

Name	Company	Comments	Drafting Team Responses
		<p>other material under this subparagraph and makes the application of this standard difficult.</p> <p>B) the cyber asset uses a routable protocol, or - Although a routable protocol is significant from the perspective of a cyber system exposed to other interconnected systems, this may not be a good indicator for a critical cyber asset. A critical cyber asset should be identified based on its impact on the power system or the business functions of the responsible entity. Based upon this assessment, the risks faced by the entity (and the industry should the system be compromised) can be established. The vulnerabilities presented by the use of a particular protocol can then be examined in the context of exposure (e.g., the use of a routable protocol on an isolated minor system whose compromise would have little business impact, does not qualify it for categorization as critical.)</p> <p>C) the cyber asset is dial-up accessible. Similar comment to that above. Exposure is assumed, however. Nevertheless, the impact of the system and its compromise through the exposure mechanism must be considered before the system should be categorized as critical. In addition, mitigating controls, such as dial-up through a private branch exchange or the employment of dial-back technology must be considered.</p> <p>D) Dial-up accessible critical cyber assets, which do use a routable protocol require only an electronic security perimeter for the remote electronic access without the associated physical security perimeter.</p>	
Denis Kalma	AESO	<p>1302.a.1 Suggest use of Interconnection rather than electric grid for consistency among other reliability standards.</p> <p>The FAQ doesn't reflect this section very well. FAQ should better define the electronic perimeter in substations.</p>	<p>The phrase "operation of the interconnected bulk electric system" is in the revised section 1302. A standard definition for BES is in the Version 0 Glossary of Terms.</p> <p>Modifications have been made to the FAQ.</p>

Name	Company	Comments	Drafting Team Responses
Ed Goff	Progress Energy	<p>1302 Critical Cyber Assets - a - using their own preferred risk based assessment -- seems to encourage inconsistency..."bring me a rock...another." Lists of standard methodologies or equivalent should be required. BCI? --</p> <p>a.1.ii - Definition of IROL should appear in Definitions or Glossary sections. Also, could more specific criteria be defined to assist in determining what should be classified as critical?</p> <p>- a.1.v - Is this intended to include demand side management systems which shed Distribution loads?</p> <p>- a.3 - i.3.iv - Requiring senior management officer approval of bulk electric system assets and cyber asset lists implies that as equipment is changed it must be approved by senior management officer. This appears to be excessive documentation and record keeping which does not seem to balance the effort and costs required given the security benefits. Also, this LOE will like require dedicated staff.</p> <p>- g.4.i -- annually -- could we use consistent time intervals? Instead of annually 12 months...there may be interpretation issues otherwise.</p>	<p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>The definition of for Interconnection Reliability Operating Limits (IROL) is a term used within other NERC documents and standards, and is well understood by BES Operations personnel. 1300 will not attempt to redefine it.</p> <p>NERC span of control does not include Distribution Systems, and they are not included.</p> <p>Senior management sign-offs are required at least annually. Senior management would not have to approve each change if a process was in place to ensure that changes to critical assets or cyber critical cyber assets are managed and documented within 30 days of the change.</p> <p>With regards to 1302.4, Compliance Monitoring, the section has been modified to be clearer with regards to what must actions must occur on what cycle – i.e.; 30 days, six months, one calendar year, three calendar</p>

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

years. It is also re-drafted to be clearer has to what data must be retained, and for how long..

Name	Company	Comments	Drafting Team Responses
Ed Riley	CAISO	<p>1302.a This paragraph should be rephrased to provide clearer meaning. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence were stated first, this may be clearer.</p> <p>1302.a.1 Replace "electric grid" with "critical bulk electric system" for consistency.</p> <p>1302.a.2 FORMATTING/NUMBERING ISSUE</p> <p>(i) The responsible entity shall identify cyber assets to be critical using the following criteria:</p> <p>A) The cyber asset supports a critical bulk electric system asset, and</p> <p>i) the cyber asset uses a routable protocol, or</p> <p>ii) the cyber asset is dial-up accessible.</p> <p>B) Dial-up accessible critical cyber assets, which do use a routable protocol require only an electronic security perimeter for the remote electronic access without the associated physical security perimeter.</p> <p>1302.a.2.3 The term "senior management" and "officer" have legal meaning in many companies, it should be clarified further of what is level of authority is necessary.</p> <p>Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>



Name	Company	Comments	Drafting Team Responses
			<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>The standard does not preclude grouping of assets by category provided each asset is also listed.</p>

Name	Company	Comments	Drafting Team Responses
Ed Stein	FirstEnergy	<p>1302 -- Critical cyber assets</p> <p>Page 10: Critical Cyber Assets: "...the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.</p> <p>Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.</p> <p>ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis &amp; Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits.</p> <p>ABC seeks clarification on the following:</p> <p>ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis &amp; Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.</p> <p>ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.</p> <p>ABC seeks clarification of the 'dial up accessible' reference</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>regarding DNP.</p> <p>Is an electronic relay interpreted by NERC to be a computerized cyber asset?</p> <p>If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?</p> <p>Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".</p> <p>Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.</p> <p>Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.</p> <p>ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "...greater than or equal to 80% of the most severe single contingency loss."</p> <p>ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:</p> <p>Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR</p> <p>Same utility owns 100 % of a 635 MW generation site</p> <p>Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>The use of terms like "control" and "support" imply that if the loss or compromise of the cyber asset has significant negative impact on maintaining reliable operation of the BES, and is accessible via a routable protocol or dial-up, then it is a critical cyber asset.</p> <p>The terms "routable protocol" and "dual-up" are well understood by information technology professionals and should not need further definition. If you have an otherwise critical cyber asset, but it does not use a routable protocol or dial-up for access, then it does not need to comply 1300.</p> <p>Depending on its configuration, an electronic relay and its associated electronic files might be a cyber asset.</p> <p>The previously referenced policies are becoming NERC standards. Their new designations will be referenced in the future. Where NERC standards already (including Version Zero) make accommodation for Regional differences, those differences will apply. They should not be re-stated, or stated differently, in 1300. To state it specifically, could cause conflicts if, for example the standard for Reporting Differences is modified in the future.</p> <p>In section 1302 the generation criteria has been changed to "...80% of greater of the largest single contingency within the Regional Reliability</p>

Name	Company	Comments	Drafting Team Responses
		<p>"critical cyber assets."</p> <p>ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).</p> <p>Page 9: Either fully explain or eliminate (iii) Generation (B) "...generating resources that when summed meet the criteria..."</p> <p>Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) "...A sr. management officer must approve the list of..." and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.</p> <p>In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.</p>	<p>Organizations."</p> <p>We see no question associated with the development of a list of Critical BES Assets (including functions and tasks), and a list of Critical Cyber Assets. We see nominal cost associated with assigning fiduciary responsibility for management sign-off assuring the list is valid. There are few if any other sign-off requirements.</p> <p>FAQs further explain joint owned units and "...generation resources that when summed meet the criteria...".</p> <p>Ensuring that senior management are directly involved in the cyber security program is an important aspect of the standard.</p> <p>If the webcast was misleading, we apologize. 1300, and 1302 specifically, make no reference to three steps.</p>

Name	Company	Comments	Drafting Team Responses
Francis Flynn	National Grid	<p>Replace the 1302 introduction and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, the responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Previous section 1302.g has been re-drafted as suggested.</p>

Name	Company	Comments	Drafting Team Responses
		<p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p> <p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval"</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of</p>	

Name	Company	Comments	Drafting Team Responses
		<p>the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302; "critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	
Francois Lemay	Brascan Power	<p>Clear up ambiguity of section 1302.a.2.i that says 'A and B or C' by specifying if you mean 'A and (B or C)' or you mean '(A and B) or C'</p>	This is addressed in the re-drafting.



Name	Company	Comments	Drafting Team Responses
Gary Campbell		<p>1302:</p> <p>Requirements:</p> <p>The word inventory in the first paragraph seems to mean action. Rewording so as to require documentation of this inventory may be more appropriate</p> <p>There is no requirement to update the lists and I believe this would an important part of the process.</p> <p>Measures:</p> <p>What does "a properly dated" record mean in #5 ? Could be omitted?</p> <p>Levels of non-compliance:</p> <p>The level description should be more explicit. Many questions and uncertainty can arise when terms like "required documents" and "known changes" are used to define what the CM is to look for. Also, how is the CM to know if he has classified all the right documents as required. It should not be up to the CM to make these decisions.</p> <p>Level 3 and 4 seem to be imbalanced? If I have one document missing out of, let's say 7 documents, I will be level 3 but if I don't do anything I am level 4.</p>	<p>So noted and addressed in re-drafting under measures.</p> <p>"properly dated" should read as, Signed and dated ...</p> <p>Re-drafting will initiate changes to these sections.</p>
Greg Fraser	Manitoba Hydro	In section 1302 (a) (1) (vi) remove the redundant word ...negatively..	Done

Name	Company	Comments	Drafting Team Responses
Guy Zito	NPCC	<p>Standard 1300 is based on what the critical BES assets are, which is defined in 1302.a.1. Per question 1, NPCC's participating members do not agree with that definition and have made suggestions as to what the Drafting Team may do to address the issue.</p> <p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p> <ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul> <p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets</p> <p>(i) The responsible entity shall maintain its critical bulk electric</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Previous section 1302.g has been re-drafted as suggested.</p>

Name	Company	Comments	Drafting Team Responses
		<p>system assets approved list as identified in 1302.1.1."</p> <p>to</p> <p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p> <p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more</p>	

Name	Company	Comments	Drafting Team Responses
		<p>appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302;</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	
Howard Ruff	WE Energies	Section 1302, Critical Cyber Assets item 2 (D). Please clarify what is meant here. Does this statement mean a computer that is used to access a critical cyber asset via remote access (dial up) does not have to be included in the physical perimeter? Also, in the same section under measures, risk based assessment, the current NERC risk evaluation standard should be referenced as a guide.	Computers used to access a critical cyber asset via remote access (dial up) will require an electronic security perimeter but they may not require a physical security perimeter?
Jim Hiebert	WECC EMS WG	1302.a.3 Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.	The standard does not preclude grouping of assets by category provided each asset is also listed.

Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>1302 -- Critical cyber assets</p> <p>Page 10: Critical Cyber Assets: "...the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.</p> <p>Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.</p> <p>ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis &amp; Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits.</p> <p>ABC seeks clarification on the following:</p> <p>ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis &amp; Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.</p> <p>ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.</p> <p>ABC seeks clarification of the 'dial up accessible' reference</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>regarding DNP.</p> <p>Is an electronic relay interpreted by NERC to be a computerized cyber asset?</p> <p>If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?</p> <p>Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".</p> <p>Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.</p> <p>Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.</p> <p>ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "...greater than or equal to 80% of the most severe single contingency loss."</p> <p>ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:</p> <p>Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR</p> <p>Same utility owns 100 % of a 635 MW generation site</p> <p>Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>The use of terms like "control" and "support" imply that if the loss or compromise of the cyber asset has significant negative impact on maintaining reliable operation of the BES, and is accessible via a routable protocol or dial-up, then it is a critical cyber asset.</p> <p>The terms "routable protocol" and "dual-up" are well understood by information technology professionals and should not need further definition. If you have an otherwise critical cyber asset, but it does not use a routable protocol or dial-up for access, then it does not need to comply 1300.</p> <p>Depending on its configuration, an electronic relay and its associated electronic files might be a cyber asset.</p> <p>The previously referenced policies are becoming NERC standards. Their new designations will be referenced in the future. Where NERC standards already (including Version Zero) make accommodation for Regional differences, those differences will apply. They should not be re-stated, or stated differently, in 1300. To state it specifically, could cause conflicts if, for example the standard for Reporting Differences is modified in the future.</p> <p>In section 1302.1.1.3 the generation criteria has been changed to "...80% of greater of the largest single contingency within the Regional Reliability</p>

Name	Company	Comments	Drafting Team Responses
		<p>"critical cyber assets."</p> <p>ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).</p> <p>Page 9: Either fully explain or eliminate (iii) Generation (B) "...generating resources that when summed meet the criteria..."</p> <p>Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) "...A sr. management officer must approve the list of..." and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.</p> <p>In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.</p>	<p>Organizations."</p> <p>We so no question associated with the development of a list of Critical BES Assets (including functions and tasks), and a list of Critical Cyber Assets. We see nominal cost associated with assigning fiduciary responsibility for management sign-off assuring the list is valid. There are few if any other sign-off requirements.</p> <p>FAQs further explain joint owned units and "...generation resources that when summed meet the criteria..."</p> <p>Ensuring that senior management are directly involved in the cyber security program is an important aspect of the standard.</p> <p>If the webcast was misleading, we apologize. 1300, and 1302 specifically, make no reference to three steps.</p>



Name	Company	Comments	Drafting Team Responses
Joe Weiss	KEMA	1302.a.2.i.D should read Dial-up accessible critical cyber assets, which to not use a routeable protocol. The not is missing.	Corrected in the re-draft.
John Blazeovitch	Exelon	<p>1302.a.3 Responsibility for critical bulk electric system assets and critical cyber assets is likely to be shared between multiple business units. We recommend that this requirement read: At least one senior management official...</p> <p>1302.a.2.i.A For emphasis, we recommend underlining and.</p> <p>1302.g.1.i For clarity, we recommend that the sentence read: The responsible entity shall maintain its approved list of critical bulk electric systems assets as identified under...</p>	<p>It is expected that someone from Operations will sign-off on the BES list, and someone from IT will sign-off on the Critical cyber assets list.</p> <p>The NERC standards templates do not allow for underline formatting.</p> <p>Agreed.</p>

Name	Company	Comments	Drafting Team Responses
John Hobbick	Consumers Energy	<p>1302 -- Critical Cyber Assets</p> <p>1) Critical Bulk Electric System Assets</p> <p>Our understanding is that the selection of critical facilities is based on each entities risk assessment. The list of facilities included in the standard is meant as a starting point in preparing the risk assessment and does not mean that those facilities have to be on your critical list.</p> <p>The risk assessment process should allow for the extent in which cyber assets control a critical bulk electric facility (i.e. a large substation with a limited number of dial up accessible relays) while the substation may be critical, the cyber assets are not</p> <p>iii)Clarification of the use of disturbance reporting NERC Policy 1B Section 2.4 as a selection criteria for generation:</p> <p>a. Some Reliability Councils have added additional criteria to disturbance reporting</p> <p>b. What is the impact of particiapating in a reserve sharing group</p> <p>2) Critical Cyber Assets</p> <p>A. Should be worded The cyber asset controls a critical bulk electric system asset</p> <p>D For remote locations such as substations, in addition to dial up access only requiring an electronic perimeter, properly secured devices with a routable protocol should not require or have limited requirements for physical security. The ability to physically secure devices at an unmanned substation is limited and should be used in conjunction with electronic security. Also the ability to physically secure a substation control house or cage at the same level as a control center or computer room is not realistic. Background screening and logging all entrances would be expensive or difficult to enforce.</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose their preferred methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the</p>

Name	Company	Comments	Drafting Team Responses
			<p>minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as “high-jacking” or “day zero attacks.” While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of essential BES and critical cyber assets.</p>
John Lim	Con Ed	<p>1302: A definition of what constitutes a bulk electric system asset and what makes it critical must be clear enough to allow responsible entities to identify it. Con Edison believes that the definition of "bulk electric system" and "critical bulk electric asset" is outside the scope of a cyber security standard. Wording such as "as defined by NERC and the applicable regional reliability coordinating organization" can be used to defer the definition of these to the appropriate group within NERC and the regions. The FAQ can provide additional clarifications based on current definitions or work in progress in NERC.</p>	Agreed

Name	Company	Comments	Drafting Team Responses
Karl Tammer	ISO-RTO Council	<p>1302.a This paragraph would be clearer if it were rephrased. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence were stated first, this would be clearer.</p> <p>1302.a.1 Replace "electric grid" with "bulk electric system" for consistency.</p> <p>1302.a.3 The terms "senior management" and "officer" have legal meaning in companies. This should be clarified further.</p>	<p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>"A senior management officer" should read "a member of senior management".</p>

Name	Company	Comments	Drafting Team Responses
Kathleen Goodman	ISO_NE	<p>1302 PREAMBLE: There is great concern that reference to bulk electric system assets, and those assets deemed critical, is addressing the physical security of those assets. This must be clarified as physical security of BES assets does NOT belong in a cyber security standard.</p> <p>Suggest rewriting as: "Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>"The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks."</p> <p>1302 Requirements: This paragraph would be clearer if it were rephrased. By commencing with the first sentence, it could be interpreted that the standard may be intending to speak to protection methods around bulk electric systems when it is only the cyber systems. If the second sentence was stated first, this would be clearer.</p> <p>Suggest rewriting as: "Responsible entities shall identify their Critical Cyber Assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard."</p> <p>(1) Rewrite as:</p>	<p>References to BES assets and critical BES assets is only to obtain the critical cyber asset list. Then the associated physical security only applies to the critical cyber assets</p> <p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support</p>

Name	Company	Comments	Drafting Team Responses
		<p>"(1) Critical Bulk Electric System Operating Functions and Tasks The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system operating at the levels of 115 kV and above. Critical operating functions and tasks affected by cyber assets may include but are not limited to the following:</p> <ul style="list-style-type: none"> <li>- monitoring and control</li> <li>- load and frequency control</li> <li>- emergency actions</li> <li>- contingency analysis</li> <li>- arming of special protection systems</li> <li>- power plant control</li> <li>- substation control</li> <li>- real-time information exchange"</li> </ul> <p>(2) Critical Cyber Assets: Rewrite as: "In determining the set of Critical Cyber Assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <ul style="list-style-type: none"> <li>- The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</li> <li>- The consequences of the Operating Function or Task being compromised (i.e. "high-jacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</li> <li>- Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</li> <li>- Known risks associated with particular technologies."</li> </ul> <p>The criteria nesting/indents is confusing. Rephrase to read as: (i) The responsible entity shall identify cyber assets to be critical using the following criteria: B) The cyber asset supports a critical bulk electric system asset, and i) the cyber asset uses a routable protocol, or</p>	<p>this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>"A senior management officer" should read "a member of senior management".</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of essential BES and critical cyber assets.</p> <p>Recommendations for Measures section will be addressed with the re-write.</p>

Name	Company	Comments	Drafting Team Responses
		<p>ii) the cyber asset is dial-up accessible.</p> <p>C) Dial-up accessible Critical Cyber Assets, which do use a routable protocol require only an electronic security perimeter for the remote electronic access without the associated physical security perimeter.</p> <p>(3) The terms "senior management" and "officer" have legal meaning in companies. This should be clarified throughout the standard.</p> <p>1302 Measures:</p> <p>(1) Rewrite as:</p> <p>"(1) Critical Bulk Electric System Operating Functions and Tasks</p> <p>(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.Requirements.1."</p> <p>(2) Rewrite as:</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its Critical Cyber Assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>(5) Change title to: "Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval"</p> <p>(5.i) through (5.ii) This should read as, senior Operating System Manager</p>	

Name	Company	Comments	Drafting Team Responses
Ken Goldsmith	Alliant Energy	<p>1302 Critical Cyber Assets</p> <p>Article a-1 and 2 The definitions of bulk electric system facility, critical cyber asset and IROL should be moved to the Definitions section. Other clarification is needed regarding telemetry and common system under Generation</p> <p>Article a-2-E Remove the statement: Any other cyber asset within the same electronic security perimeter as the critical cyber assets must be protected to ensure security of critical cyber assets. Having to comply with each section of this standard for a non-critical asset is too burdensome. Suggest a reference in Section 1306 to ensure non-critical cyber assets within the same electronic perimeter have appropriate controls to protect the critical asset.</p>	<p>Bulk Electric System, Interconnection Reliability Operating Limits (IROL), and Reporting Disturbances (RD) are NERC defined terms, which exist in other NERC standards and glossaries. Where IROL and RD exist in other standards, regional differences are addressed within those standards as well. 1300 will not attempt to further define these terms.</p> <p>Cyber assets sharing an open (homogeneous) network environment -- i.e., inside the same electronic perimeter -- can put other critical cyber assets at risk and therefore must be protected equally.</p>



Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	<p>Section 1302</p> <p>The terms "critical cyber assets" and "critical bulk electric system assets" are defined differently within this section (compare opening paragraph and parag. [a][1]), and both are different from that used in the Definitions Section. Moreover, the FAQ says that there is no definition. The standard should use one definition, in particular the CIPC-approved definition. See comments at Definitions Section.</p> <p>(a)(1)(i)(A) --</p> <p>Clarify that "telemetry" does not include "telecommunication" equipment.</p> <p>Check formatting and revise/correct as necessary.</p> <p>(a)(1)(ii) -- Move this subsection to the Definitions Section (revise and renumber format).</p> <p>(a)(1)(iii) --</p> <p>This subsection raises a number of complicated issues (especially applicable to voltage support):</p> <p>Does "generating resources" include physical and market resources?</p> <p>If it includes market resources, how is a determination by the buyer that a resource is critical to be communicated to the seller and/or generator?</p> <p>What if they do not agree to such a designation?</p> <p>How is their performance to be evaluated, and by whom?</p> <p>Who has responsibility for the electronic or physical perimeter (or how is it determined) if the perimeter includes assets from both a</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		transmission and a generator owner?	
		Define the term "common system" -- its meaning is not clear from the context alone.	essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.
		(a)(1)(iv)(B) -- What is meant by the term "initial"? Its meaning is not clear from the context alone.	In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.
		(a)(1)(v) -- Define the term "common system" -- its meaning is not clear from the context alone.	
		(a)(1)(vii)(A) --	We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.
		The standard needs to clearly and explicitly exclude nuclear assets.	
		Check formatting and revise/correct as necessary.	
		(a)(2)(i)(A) --	
		Underline "and" to emphasize it, as it is important and could be overlooked with the existing formatting.	Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of essential BES and critical cyber assets.
		Check formatting and revise/correct as necessary.	
		(a)(2)(i)(D) --	
		Appears to have dropped a negative: the operative clause should read "which do not use a routable protocol."	Telemetry does not include telecommunication equipment.
		It would be better, however, to revise the phrase to read "which use an insecure routable protocol," as the original concept is too restrictive (even correcting the missing negative -- see above). Inclusion of all assets that use routable protocols is excessive -- only those that use such protocols and are also connected to the Internet or a public telecommunications network should be included. The implication in the proposed draft is that non-routable protocols are more secure than routable protocols when used for communications with substation equipment. This is not correct. Even non-routable	NERC and 1300 scope only address BES assets, functions, and tasks. Market specific assets and functions are included by definition. However, consideration must be given to systems that might support dual functionality. The focus of the cyber security standard is assets critical to the operation of the interconnected bulk electric system.
			If multiply-owned/operated assets reside with a common perimeter, a business agreement on designation of responsibilities must be worked-out by

Name	Company	Comments	Drafting Team Responses
		<p>protocols can be exploited with readily available technology. A modern, properly secured routable protocol connection (using at a minimum encryption and certificates) is significantly more secure than legacy non-routable protocols. (Legacy protocols, while proprietary, have been in use in many cases over thirty years worldwide, and documentation was widely disseminated. When they were developed, most of these legacy protocols required special hardware to implement, but today can be emulated easily using software. Various methods can be used to impose malicious traffic on a circuit.) Since most of the cyber equipment installed in substations is embedded, applying the proposed standard will have little effect. Also, the equipment was not designed with security or versatility in mind, and cannot be upgraded easily or just for security reasons. The proper way to protect these (generally substation) assets is to secure the communications paths to them, rather than to impose control-center type security methods on them. The standard should simply address the point of vulnerability -- the communications interface -- and insure that is secured.</p> <p>Check formatting and revise/correct as necessary.</p> <p>(a)(2)(i)(E) --</p> <p>The reference to "1302.1.2.1." does not appear to be matched to any text.</p> <p>Check formatting and revise/correct as necessary.</p> <p>Consider moving this subsection to Section 1306, as "other" cyber assets are not critical assets even when located within a security perimeter, and their protection could be considered part of overall system security management.</p> <p>(g)(1)(i) --</p> <p>The reference to "1302.1.2.1." does not appear to be matched to any text.</p>	<p>all parties.</p> <p>Common in this context means "shared by or belonging to all".</p> <p>"Initial" restoration versus complete system restoration.</p>

Name	Company	Comments	Drafting Team Responses
		Check formatting and revise/correct as necessary.	
		(g)(3)(i) --	
		The reference to "1302.1.2.1." does not appear to be matched to any text.	
		Check formatting and revise/correct as necessary.	

Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>1302 -- Critical cyber assets</p> <p>Page 10: Critical Cyber Assets: "...the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". Cinergy recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.</p> <p>Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, Cinergy has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to Cinergy's Energy Management System.</p> <p>Cinergy interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis &amp; Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits.</p> <p>Cinergy seeks clarification on the following:</p> <p>Cinergy currently uses a "non-routable" protocol (e.g. Cinergy's current Landis &amp; Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. Cinergy seeks clarification on routable protocol reference and how NERC believes it applies here.</p> <p>Cinergy needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.</p> <p>Cinergy seeks clarification of the 'dial up accessible' reference</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>regarding DNP.</p> <p>Is an electronic relay interpreted by NERC to be a computerized cyber asset?</p> <p>If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?</p> <p>Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".</p> <p>Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all Cinergy's generating facilities fall under the rules of Standard 1300.</p> <p>Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.</p> <p>Cinergy recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "...greater than or equal to 80% of the most severe single contingency loss."</p> <p>Cinergy seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:</p> <p>Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR</p> <p>Same utility owns 100 % of a 635 MW generation site</p> <p>Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which Cinergy does not consider critical, will be included in the list of</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>The use of terms like "control" and "support" imply that if the loss or compromise of the cyber asset has significant negative impact on maintaining reliable operation of the BES, and is accessible via a routable protocol or dial-up, then it is a critical cyber asset.</p> <p>The terms "routable protocol" and "dual-up" are well understood by information technology professionals and should not need further definition. If you have an otherwise critical cyber asset, but it does not use a routable protocol or dial-up for access, then it does not need to comply 1300.</p> <p>Depending on its configuration, an electronic relay and its associated electronic files might be a cyber asset.</p> <p>The previously referenced policies are becoming NERC standards. Their new designations will be referenced in the future. Where NERC standards already (including Version Zero) make accommodation for Regional differences, those differences will apply. They should not be re-stated, or stated differently, in 1300. To state it specifically, could cause conflicts if, for example the standard for Reporting Differences is modified in the future.</p> <p>In section 1302.1.1.3 the generation criteria has been changed to "...80% of greater of the largest single contingency within the Regional Reliability</p>

Name	Company	Comments	Drafting Team Responses
		<p>"critical cyber assets."</p> <p>Cinergy recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).</p> <p>Page 9: Either fully explain or eliminate (iii) Generation (B) "...generating resources that when summed meet the criteria..."</p> <p>Page 10: Cinergy believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. Cinergy has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. Cinergy recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) "...A sr. management officer must approve the list of..." and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.</p> <p>In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. Cinergy seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.</p>	<p>Organizations."</p> <p>We so no question associated with the development of a list of Critical BES Assets (including functions and tasks), and a list of Critical Cyber Assets. We see nominal cost associated with assigning fiduciary responsibility for management sign-off assuring the list is valid. There are few if any other sign-off requirements.</p> <p>FAQs further explain joint owned units and "...generation resources that when summed meet the criteria..."</p> <p>Ensuring that senior management are directly involved in the cyber security program is an important aspect of the standard.</p> <p>If the webcast was misleading, we apologize. 1300, and 1302 specifically, make no reference to three steps.</p>

Name	Company	Comments	Drafting Team Responses
Laurent Webber	WAPA	<p>Section 1302, Critical Cyber Assets, (a)(1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).</p> <p>Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station and, therefore, carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?</p> <p>Section 1302, Critical Cyber Assets, (a)(2). The logistics for items A-E should be clarified; it is confusing.</p> <p>Section 1302, Critical Cyber Assets, (a)(2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter and what does not). Is there a typo in 1302(a)(2)(i)(D): it reads, "which do use a routable protocol," should is say "which do NOT use a routable protocol"?</p>	<p>The criteria in Section 1302.a.1.iii is changed to "...80% or greater of the largest single contingency within the Regional Reliability Organization."</p> <p>The logistics for items A-E in Section 1302, Critical Cyber Assets, (a)(2) has been corrected and clarified.</p>
Linda Nappier	Ameren	<p>1302 (a) (1) (iii) A) Reportable Disturbance -- Does the reportable disturbance limit include reserve sharing groups?</p>	<p>The criteria in Section 1302.a.1.iii is changed to "...80% or greater of the largest single contingency within the Regional Reliability Organization."</p>



Name	Company	Comments	Drafting Team Responses
Lloyd Linke	WAPA - MAPP	<p>1302 Critical Cyber Assets, (a) (1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).</p> <p>Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station, and therefore carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?</p> <p>1302 Critical Cyber Assets, (a) (2). The logistics for Items A-E should be clarified; it is confusing.</p> <p>1302 Critical Cyber Assets, (a) (2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter, and what does not?). Is there a typo in 1302 (a) (2) (i) (D): it reads "which do use a routable protocol" - should say "which do NOT use a routable protocol"?</p>	<p>The criteria in Section 1302.a.1.iii is changed to "...80% or greater of the largest single contingency within the Regional Reliability Organization."</p> <p>The logistics for items A-E in Section 1302, Critical Cyber Assets, (a)(2) has been corrected and clarified.</p>

Name	Company	Comments	Drafting Team Responses
Lyman Schaeffer	Pacific Gas & Electric	<p>Section 1302: Critical Cyber Assets :</p> <p>We again noted the inclusion of telemetry within the areas of concern and want to stress, as we did in the definition section, that this should not broadly include the company's telecommunications network.</p> <p>We appreciate the standard providing flexibility for each company to use a self determined risk assessment to identify its critical cyber assets. However, as reflected in our subsequent comments, the standard does not seem to give the company the ability to design its security program based on the results of that assessment.</p> <p>Our major concern in this section is the inclusion of a routable protocol within the parameters of this standard. While we understand the concerns regarding a protocol connected or easily accessible to the internet, we believe that a routable protocol that is isolated from the internet should be specifically exempted from this standard. Moreover, each company should use their risk assessment to determine what level of security is acceptable regardless of whether a specific device qualifies as being routable.</p>	<p>Telemetry does not include telecommunication equipment. Telecommunications is not covered by the cyber security standard.</p> <p>Routable protocols in the criteria to determine critical cyber assets limits the implementation of the cyber security standard to those cyber assets which potentially have increased risk exposure to cyber threats.</p>

Name	Company	Comments	Drafting Team Responses
Neil Phinney	Georgia Transmission Co	<p>1302.a.2 The Label of an asset as "critical" should be based on its function, not the communication method it uses. Use of a routable protocol may be one of several characteristics that make a device vulnerable, but it does not bear on the issue of whether a device is critical. This section even contradicts the definition in 1300 itself. The definition specifically includes devices that perform monitoring and control (presumably RTUs), but 1302 indicates that they would be included only if they use a routable protocol. Why should a device connected to a Bulk Electric System Facility be a critical asset if it uses the IP protocol to connect to the device, and not be critical if it performs the same function using a serial protocol? Whether a device is critical should depend on its function, not the protocol used or even the type of communication (dedicated or switched) to perform that function.</p> <p>1302.a.2 Routable protocol networks vary dramatically and should not all be treated the same. Routable protocol networks can range from the public Internet to an isolated, two-node, point to point link. To treat these networks the same from a security standpoint is illogical, but is exactly what section 1302 (a)(2) does. The level of protection needed to secure communication should be based on the overall character of the network, not simply on the protocol it uses. Whether a routable protocol is used is one characteristic, but by itself tells almost nothing about the character of the network. We would suggest that the criteria of whether the network has a routable connection to a public network might be a more appropriate threshold test. 1302.a.2.I.D Is there a misprint in regarding the "dial-up accessible critical cyber assets" in this section? The section refers to dial-up accessible cyber assests that DO use routable protocols, which contrasts the answer to question #6 pertaining to section 1302 of the "Cyber Secuity Standard 1300 Frequently Asked Questions (FAQ's) identifying dial-up accessible cyber assests that DO NOT use routable protocols.</p> <p>1302a2Serial radio based networks present a comparable or greater risk than many routable protocol networks and should be treated similarly. Radio based networks, because their communication path is open to all listeners (and talkers) in a wide geographic area represent a substantial risk to cyber security. The ease with which</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>an outside party could intercept a utility transmission or substitute his own transmission for the utility transmission is frightening. This risk far exceeds that of an isolated IP based segment. Yet 1302 excludes the radio system while including the IP segment.</p> <p>1302a2IDThis paragraph seems to require a less stringent security standard for systems that use dial-up routable protocols (no physical perimeter) than for dedicated service. We can't see a justification for this. There is a conflict between the text of the standard and the text in the portion of the FAQ referring to this section. The standard refers to dial-up connections that DO use a routable protocol, while the FAQ refers to dial-up connections that DO NOT. Perhaps there is a typo.</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>Routable protocols in the criteria to determine critical cyber assets limits the implementation of the cyber security standard to those cyber assets which potentially have increased risk exposure to cyber threats.</p> <p>Typo corrected in 1302.a.2.i.D.</p>

Name	Company	Comments	Drafting Team Responses
Paul McClay	Tampa Electric Company	<p>1302 Critical Cyber Assets</p> <p>(a) (1) (ii) The standard is referring to a term (IROL) that is not currently an approved term within the NERC operating policies. Is it the drafting team's assumption that this definition will be a part of the NERC policy by the time this standard is implemented, or will this definition and related definitions from the FAQ be included in the definitions for this standard?</p> <p>(a) (1) (iii) (A) Reportable Disturbance criteria Within a generating station, each unit may be controlled by separate non-connected distributed control systems but may be under the control of a common automated generation control (AGC) system from an energy control center. Does AGC qualify as a common system controlling generating resources for the purposes of this standard? If so, does the AGC need to be routable (TCP/IP) to make these resources qualify as critical cyber assets? We feel this should be clarified in the standard.</p> <p>(a) (2) (i) (A) Critical Cyber Assets: Revise From: The cyber asset supports a critical bulk electric system asset, and" To: The cyber asset affects the reliability and operation of a critical bulk electric system asset, and"</p> <p>Add to: 1302 (a) (2) (i) as new item: An isolated routable network (i.e. closed IP network) located in a secure area that is not connected to a modem and has no other means of external access shall be considered a non-critical cyber asset. As a note, in the conference call of October 18th, Larry Bugh agreed with the person who suggested this. (See Question 5f in the summary of Q&amp;A)</p> <p>(a) (2) (i) E -- the reference (1302.1.2.1) doesn't exist. Similar references that don't point to anything in this document appears in 1302 (g) (1) (i), (g) (3) (i), (g)(4) (i).</p>	<p>The standard refers to a term (IROL) that is not currently an approved term within the NERC operating policies or approved standard. If this definition is not part of the NERC standards or definition by the time this standard is implemented, then this definition and related definitions from the FAQ will be included in the definitions for this standard.</p> <p>If the common AGC affects generation meeting the criteria for critical assets and critical cyber assets, then this control would be required protection under the cyber security standard.</p> <p>In 1302 the critical cyber asset section has been revised.</p> <p>The comments during the webcast on October 18th were in error. An isolated system using a routable protocol within an electronic security perimeter must be secured according to the cyber security standard.</p> <p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>Cyber assets sharing an open (homogeneous) network environment -- i.e., inside the same electronic perimeter -- can put other critical cyber assets at risk and therefore must be protected equally.</p>

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

(a) (2) (i) E -- refers to other cyber assets in same electronic security perimeter needing to be "protected" but section 1302 only addresses making lists. Should other cyber assets in the perimeter be on the lists? Why? The protection of those assets should be covered elsewhere, if they need to be protected at all. If they don't impact the running of critical bulk electric facilities, why do they need to be protected?

Name	Company	Comments	Drafting Team Responses
Peter Burke for Dave Mueller	ATC	<p>On page 10 under the section Critical Cyber Assets item (B) which currently reads:</p> <p>"the cyber asset uses a routable protocol, or"</p> <p>should be changed to:</p> <p>"the cyber asset uses a non secure routable protocol, or"</p> <p>With this change the standard can achieve the desired goal of insuring that critical assets are secure without imposing a severe burden on those companies that installed modern equipment in their substations while rewarding those companies that have continued to use old legacy equipment. The implication in the current draft of the standard that non routable protocols are more secure than routable protocols when used for communications with substation equipment is not correct. While routable protocols are typically attacked by hackers the non routable legacy protocols are very easy for someone to exploit with readily available technology. These protocols while proprietary have been in use in many cases for over thirty years worldwide. Before security concerns changed documentation on these protocols was readily disseminated. When they were developed most of these legacy protocols required special hardware to implement. With today's PCs the protocols can be emulated easily using only software. Various methods can be used to impose malicious traffic on a circuit causing major problems on the electric system. A properly secured routable protocol connection to the substation using at a minimum encryption and certificates is significantly more secure than the legacy protocols. The standard should be written to encourage companies to install new systems that improve security, not encourage them to leave vulnerable legacy equipment in place. Since most of the cyber equipment installed in substations are embedded equipment applying the cyber standards have little effect. The equipment cannot be upgraded for security issues and was not designed with security concerns in mind. The proper way to protect these assets is</p>	<p>Section 1302.a.2.i.B is written correctly as "the cyber asset uses a routable protocol, or". Even if the routable protocol is secured the critical cyber asset must be identified and secured according to all sections of the standard.</p>

Name	Company	Comments	Drafting Team Responses
		<p>to secure the communications path, not to attempt to impose control center security controls on the substation equipment.</p> <p>If the goal of the standard is to improve security then the standard should apply equally to all substation sites irrespective of protocol or the standard should simply address the point of vulnerability, the communications interface, and insure that it is secured.</p>	



Name	Company	Comments	Drafting Team Responses
Ray A'Brial	CHGE	<p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p>
		1302.a.1.i.A Clarify that telemetry does not include telecomm equipment.	
		1302.a.1.ii move to definitions	
		1302a.1.ii Does generating resources include physical and market resources? If it includes market resources, how is a determination by the buyer that a resource is critical to be communicated to the seller and/or generator? How is this performance to be evaluated, and by whom? This applies to voltage support. Define common system	<p>We have also declined to provide other references to items such as “high-jacking” or “day zero attacks.” While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p>
		1302.a.1.iv.B What is meant by initial?	<p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of essential BES and critical cyber assets.</p>
		1302.a.1.v - Define common system	
		1302a.1.vii.A - Needs to clearly exclude nuclear assets.	
		(2) Critical Cyber Assets	
		(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:	<p>With regards to 1302.4, Compliance Monitoring, the section has been modified to be clearer with regards to what must actions must occur on what cycle – i.e.; 30 days, six months, one calendar year, three calendar years. It is also re-drafted to be clearer has to what data must be retained, and for how long.</p>
		(a)(2)(i)(A) -- Underline and to emphasize it.	
		A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.	

Name	Company	Comments	Drafting Team Responses
		<p>B)The consequences of the Operating Function or Task being compromised (i.e. highjacked) for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>(a)(2)(i)(D) -- if kept appears to have dropped a not: should read "which do not use a routable protocol"...</p> <p>Change 1302.g.1 from;</p> <p>(a)(2)(i)(E) -- Unmatched reference to 1302.1.2.1.</p> <p>1 Critical Bulk Electric System Assets</p> <p>(i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1.</p> <p>to</p> <p>1 Critical Bulk Electric System Operating Functions and Tasks</p> <p>(i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1.</p> <p>Change 1302.g.2.i from;</p> <p>The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure.</p>	

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure</p> <p>(g)(3)(i) -- Unmatched reference to 1302.1.2.1.</p> <p>Change 1302.g.5 from;</p> <p>Critical Bulk Electric System Asset and Critical Cyber Asset List Approval</p> <p>to</p> <p>Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval (CHGE believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained.</p> <p>to</p> <p>A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained.</p>	

Name	Company	Comments	Drafting Team Responses
		<p>Change 1302; critical bulk electric system assets</p> <p>to</p> <p>critical bulk electric system operating functions and tasks</p>	

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>1302 -- Critical cyber assets</p> <p>Page 10: Critical Cyber Assets: "...the cyber asset supports a critical bulk electric system asset." Examples: Environmental and performance software supports generation assets but is not critical to continuation of power. In the 10/18 Webcast, NERC used the word "control" rather than "supports". ABC recommends that the word "supports" be changed to reflect the intent that the cyber asset is essential to continued operation of the critical bulk electric system asset, i.e., loss of that cyber assets causes loss of the critical bulk electric system asset.</p> <p>Page 10: "Critical Cyber Assets", as defined on page 10 of the draft, narrows the definition to cyber assets that "support critical bulk electric system assets" AND "uses a routable protocol" or "is dial-up accessible". Because a proper understanding of what constitutes a critical cyber asset, ABC has several questions and seeks clarification from NERC on protocols in use throughout the organization today as well as protocol proposed for the next generation of communication from remote locations to ABC's Energy Management System.</p> <p>ABC interprets Standard 1300 to exclude devices such as remote terminal units that communicate over dedicated point to point communication circuits. An example of this would include RTU's communicating via Landis &amp; Gyr 8979 RTU protocol over 4-wire dedicated Bell 3002 circuits.</p> <p>ABC seeks clarification on the following:</p> <p>ABC currently uses a "non-routable" protocol (e.g. ABC's current Landis &amp; Gyr 8979 RTU protocol) that are communicated using PVCs (private virtual circuits) over a frame relay network. ABC seeks clarification on routable protocol reference and how NERC believes it applies here.</p> <p>ABC needs clarification on 'routable protocol' reference and how requirements apply to proposed use of "DNP over IP" using frame relay.</p> <p>ABC seeks clarification of the 'dial up accessible' reference</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>regarding DNP.</p> <p>Is an electronic relay interpreted by NERC to be a computerized cyber asset?</p> <p>If a relay is constructed to allow remote data retrieval but prohibit any configuration changes, is it excluded from the requirements?</p> <p>Page 9 Generation: Proposed Standard 1300 references other documents (Policy 1) that are open to interpretation by Regional Councils. Rather than spelling out the rules for generation that needs to be considered a Critical Bulk Electric System Assets, Standard 1300 refers to another document (Policy 1.B). ECAR has modified the definition of "Most severe single contingency".</p> <p>Using the proposed Std 1300 language from the multiple documents and regional definitions mean that almost all ABC's generating facilities fall under the rules of Standard 1300.</p> <p>Is it NERC's intent that all generating stations should be subject to the rules of Standard 1300? If this is not NERC's intent, then the proposed language needs to be changed.</p> <p>ABC recommends that all of the rules for identifying the critical bulk electric system assets and the critical cyber assets should be identified in one document, rather than using multiple documents subject to regional interpretations as used in Std 1300 version 1. Recommendation: On page 9, eliminate reference to NERC Policy 1.B in (iii) (A) and replace with this language: "...greater than or equal to 80% of the most severe single contingency loss."</p> <p>ABC seeks clarification from NERC of the term "Most severe single contingency". Please use the following example:</p> <p>Utility owns approximately 600 MW of a total 1300 MW generation site all in ECAR</p> <p>Same utility owns 100 % of a 635 MW generation site</p> <p>Which of the above should be identified as the largest "single contingency"? If the 635 MW site is used, generating units, which ABC does not consider critical, will be included in the list of</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>The use of terms like "control" and "support" imply that if the loss or compromise of the cyber asset has significant negative impact on maintaining reliable operation of the BES, and is accessible via a routable protocol or dial-up, then it is a critical cyber asset.</p> <p>The terms "routable protocol" and "dual-up" are well understood by information technology professionals and should not need further definition. If you have an otherwise critical cyber asset, but it does not use a routable protocol or dial-up for access, then it does not need to comply 1300.</p> <p>Depending on its configuration, an electronic relay and its associated electronic files might be a cyber asset.</p> <p>The previously referenced policies are becoming NERC standards. Their new designations will be referenced in the future. Where NERC standards already (including Version Zero) make accommodation for Regional differences, those differences will apply. They should not be re-stated, or stated differently, in 1300. To state it specifically, could cause conflicts if, for example the standard for Reporting Differences is modified in the future.</p> <p>In section 1302.1.1.3 the generation criteria has been changed to "...80% of greater of the largest single contingency within the Regional Reliability</p>

Name	Company	Comments	Drafting Team Responses
		<p>"critical cyber assets."</p> <p>ABC recommends that a good use for the FAQ's would be to provide additional examples, including some examples using how the requirements apply to jointly owned units (JOU's).</p> <p>Page 9: Either fully explain or eliminate (iii) Generation (B) "...generating resources that when summed meet the criteria..."</p> <p>Page 10: ABC believes the level of documentation and administrative control required by proposed Standard 1300 is extensive and imposes a significant operating cost on participants. Once again, this section contains requirements without any documented evidence that the expense to implement will enhance security or that there is a relevant threat, which will be mitigated by this level of documentation. Parts of the section are redundant to other requirements. ABC has designated two company officers that are responsible for the Cyber Security Policy and implementation. "Critical Bulk Electric system Asset and Critical Cyber Asset List Approval section," requires a properly dated record of senior management officer's approval of the list of critical bulk electric system assets. ABC recommends that requirements such as this be deleted unless evidence is shown which indicates direct security benefit. Recommendation: Eliminate Requirement (a) (3) "...A sr. management officer must approve the list of..." and also eliminate corresponding "Compliance Monitoring Process" (i) (3) (iv) page 11. The senior officers are responsible for implementation of the program and should not be required to sign off on each section of the document as each section is updated.</p> <p>In the October 18 Webcast, NERC slides indicated a "3 step" approach to identifying the critical cyber assets. Standard 1300 lists (#1) Identify the Critical Bulk Electric System Assets and (#2) Identify Critical Cyber Assets. ABC seeks clarification from NERC regarding the three (3) steps referred to in the Webcast.</p>	<p>Organizations."</p> <p>We so no question associated with the development of a list of Critical BES Assets (including functions and tasks), and a list of Critical Cyber Assets. We see nominal cost associated with assigning fiduciary responsibility for management sign-off assuring the list is valid. There are few if any other sign-off requirements.</p> <p>FAQs further explain joint owned units and "...generation resources that when summed meet the criteria..."</p> <p>Ensuring that senior management are directly involved in the cyber security program is an important aspect of the standard.</p> <p>If the webcast was misleading, we apologize. 1300, and 1302 specifically, make no reference to three steps.</p>



Name	Company	Comments	Drafting Team Responses
Richard Engelbrecht	Rochester Gas & Electric	<p>Replace the 1302 preamble and 1302.a.1 and 1302.a.2 as shown below, with;</p> <p>1302 Critical Cyber Assets Business and operational demands for maintaining and managing a reliable bulk electric system increasingly require cyber assets supporting critical reliability control functions and processes to communicate with each other, across functions and organizations, to provide services and data. This results in increased risks to these cyber assets, where the loss or compromise of these assets would adversely impact the reliable operation of critical bulk electric system assets. This standard requires that entities identify and protect critical cyber assets which support the reliable operation of the bulk electric system.</p> <p>The critical cyber assets are identified by the application of a Risk Assessment procedure based on the assessment of the degradation in the performance of critical bulk electric system operating tasks.</p> <p>(a)Requirements Responsible entities shall identify their critical cyber assets using their preferred risk-based assessment. An inventory of critical operating functions and tasks is the basis to identify a list of enabling critical cyber assets that are to be protected by this standard.</p> <p>(1) Critical Bulk Electric System Operating Functions and Tasks  The responsible entity shall identify its Operating Functions and Tasks. A critical Operating Function and Task is one which, if impaired, or compromised, would have a significant adverse impact on the operation of the inter-connected transmission system. Critical operating functions and tasks that are affected by cyber assets such as, but are not limited to, the following:</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<ul style="list-style-type: none"> <li>•monitoring and control</li> <li>•load and frequency control</li> <li>•emergency actions</li> <li>•contingency analysis</li> <li>•arming of special protection systems</li> <li>•power plant control</li> <li>•substation control</li> <li>•real-time information exchange</li> </ul>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p>
		<p>(2) Critical Cyber Assets</p> <p>(i)In determining the set of Critical Cyber assets, responsible entity will incorporate the following in its preferred risk assessment procedure:</p> <p>A)The consequences of the Operating Function or Task being degraded or rendered unavailable for the period of time required to restore the lost cyber asset.</p> <p>B)The consequences of the Operating Function or Task being compromised (i.e. "highjacked") for the period of time required to effectively disable the means by which the Operating Function or Task is compromised.</p> <p>C) Day zero attacks. That is, forms of virus or other attacks that have not yet been seen by the cyber security response industry.</p> <p>D)Known risks associated with particular technologies</p> <p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p>	<p>In achieving this re-drafting, we have avoided repeating detailed listings when these lists have already been present previously.</p> <p>We have also declined to provide other references to items such as "high-jacking" or "day zero attacks." While these may certainly be potential risks and vulnerabilities, and some of the reasons for having a cyber security standard, such vulnerabilities are not relevant to determining whether the cyber asset to critical to BES reliability.</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of essential BES and critical cyber assets.</p> <p>With regards to 1302.4, Compliance Monitoring, the section has been modified to be clearer with regards to what must actions must occur on what cycle – i.e.; 30 days, six months, one calendar year, three calendar years. It is also re-drafted to be clearer has to what data must be retained, and for how long.</p>

Name	Company	Comments	Drafting Team Responses
		<p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p> <p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p>	

Name	Company	Comments	Drafting Team Responses
		<p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302; "critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	

Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p>Definition: A clearer definition to understand what assets are considered is needed for Critical Assets as it applies to Generation. Section 1302 specifies a range of assets that are considered critical. It is not clear enough. For example, the implication of Section 1302.a.1.iii.a in combination with the referenced NERC reportable incident definition is that ANY entity with even a single small generator would have that generator a critical asset since it would be the largest single generator under that entities control.</p> <p>Definition and Section 1302.a.1.iii.a: Define Under Control of a Common System and give examples; clarify how this applies with examples. Definition (Section 1302.a.1.iii.b): Define Generation Control Centers. Definition (Section 1302.a.1.iv.B): What is meant by Initial system restoration (e.g. one bus away)?</p> <p>Section 1302.a.1.vi (Page 10) and Definitions: How does a Generator Owner know if their assets are deemed a critical electric bulk system asset? What if a Transmission Owner believes a Generator Owner is a critical electric bulk system asset (e.g. voltage support for system) but the Generator Owner does not agree? Who has responsibility of the electronic or physical perimeter if the perimeter includes assets from both a Transmission Owner and a Generator Owner? Section 1302.a.2.i.C - Suggest clarifying the wording to read, The cyber asset is dial-up accessible and connected. [Further discussion suggests that this WILL apply to cyber-assets with modems if those modems are periodically connected, since for the period in which they are connected they will meet the criteria. The implication of this is that those assets will be subject to the standard and the associated access lists, controls, monitoring etc, and that the modem requires security measures such as call-back or other authentication. Does a procedure and log requiring physical disconnection of a modem telecom connection meet the security control requirements? Section 1302.a.2.i.D: The text should read, Dial-up accessible critical cyber assets, which do not use a routable... (The word Not appears to have been omitted from the original text).</p>	<p>In section 1302 the generation criteria has been changed to "...80% of greater of the largest single contingency within the Regional Reliability Organizations."</p> <p>If mulitply-owned/operated assets reside with a common perimeter, a business agreement on designation of responsibilities must be worked-out by all parties.</p> <p>Common in this context means "shared by or belonging to all".</p> <p>FAQs further explain joint owned units and "...generation resources that when summed meet the criteria...".</p> <p>"Initial" restoration versus complete system restoration.</p> <p>Typo corrected in 1302.a.2.i.D.</p>

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

---

Name	Company	Comments	Drafting Team Responses
Robert Pelligrini	United Illuminating	<p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p> <p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302;</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of critical BES assets and critical cyber assets.</p> <p>Section 1302.g.2.i has been changed to remove the word "additional".</p>
Robert Snow		<p>These standards should apply to all control rooms that have a role in performing the functions in 1302 (a) (1) (i). They would include backup facilities and secondary control rooms.</p>	<p>Section 1302 (a) (1) (i) has been modified to include backup control centers.</p>



Name	Company	Comments	Drafting Team Responses
Robert Strauss	NYSEG	<p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p> <p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302;</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of critical BES assets and critical cyber assets.</p> <p>Section 1302.g.2.i has been changed to remove the word "additional".</p>

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>1302 (Critical Cyber Assets)</p> <ul style="list-style-type: none"> <li>• (a)(iv)(B) This should be included in the substation security standards.</li> <li>• (a)(v) Would this include some facilities within generating plants such as control rooms?</li> </ul>	<p>Any suggested changes to the substation security "guideline" should be made through your Regional physical security representative on the NERC Critical Infrastructure Protection Committee.</p> <p>Section 1302 (a)(v) refers to automatic load shedding of 300 MW or greater. If this critical asset is in a generating station then it could include the control room.</p>

Name	Company	Comments	Drafting Team Responses
S. Kennedy Fell	NYISO	<p>Change 1302.g.1 from;</p> <p>"1 Critical Bulk Electric System Assets (i) The responsible entity shall maintain its critical bulk electric system assets approved list as identified in 1302.1.1."</p> <p>to</p> <p>"1 Critical Bulk Electric System Operating Functions and Tasks (i) The responsible entity shall maintain its approved list of Critical Bulk Electric System Operating Functions and Tasks as identified in 1302.a.1."</p> <p>Change 1302.g.2.i from;</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its additional critical bulk electric system assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure."</p> <p>to</p> <p>"The responsible entity shall maintain documentation depicting the risk based assessment used to identify its critical cyber assets. The documentation shall include a description of the methodology including the determining criteria and evaluation procedure." (NPCC believes the use of the word additional is of no value as used here and recommends removal).</p> <p>Change 1302.g.5 from;</p> <p>"Critical Bulk Electric System Asset and Critical Cyber Asset List Approval"</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"Critical Bulk Electric System Operating Functions and Tasks and Critical Cyber Asset List Approval" (NPCC believes that it is more appropriate to refer to operating functions and tasks as opposed to assets as the criticality of operations of operations is lost.)</p> <p>Change 1302.g.5.i from;</p> <p>"A properly dated record of the senior management officer's approval of the list of critical bulk electric system assets must be maintained."</p> <p>to</p> <p>"A properly dated record of the senior management officer's approval of the list of the Critical Bulk Electric System Operating Functions and Tasks must be maintained."</p> <p>Change 1302;</p> <p>"critical bulk electric system assets"</p> <p>to</p> <p>"critical bulk electric system operating functions and tasks"</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of critical BES assets and critical cyber assets.</p> <p>Section 1302.g.2.i has been changed to remove the word "additional".</p>

Name	Company	Comments	Drafting Team Responses
Scott McCoy	Xcel Energy	<p>1302 Critical Cyber Assets, (a) (1). The standard is not clear whether the Largest Single Contingency for a Reportable Disturbance is specifically for the Entity or the Reserve Sharing Group (as an Entity may belong to a Reserve Sharing Group).</p> <p>Question: The FAQ defines the MOST SEVERE SINGLE CONTINGENCY as the largest single generator in the system. Does this mean only a single generating unit and not a generating station? What about greater single contingency losses as represented by the transmission facilities (subs, high voltage lines) that carry aggregated power from multiple units in a single station, and therefore carry more power than any individual generators in a Reserve Sharing Group? Wouldn't those facilities then represent the most severe single contingency?</p> <p>1302 Critical Cyber Assets, (a) (2). The logistics for Items A-E should be clarified; it is confusing.</p> <p>1302 Critical Cyber Assets, (a) (2). There should be more clarification/restatement of requirements for dial-up cyber assets that do and do not support routable protocols (what requires a physical perimeter and what does not, and what requires an electronic perimeter, and what does not) - is there a typo in 1302 (a) (2) (i) (D): it reads "which do use a routable protocol" - should say "which do NOT use a routable protocol"?</p> <p>All required minimum review periods should be a standard period of one year. Having so many review periods and having numerous periodicities is not practicable.</p>	<p>The criteria in Section 1302.a.1.iii is changed to "...80% or greater of the largest single contingency within the Regional Reliability Organization."</p> <p>The logistics for items A-E in Section 1302, Critical Cyber Assets, (a)(2) has been corrected and clarified.</p>
Seiki Harada	BC Hydro	Regarding 1302, (i) (1), change the wording to reflect that the compliance monitor may also use scheduled on-site visits of no more frequently than every three years.	This is a NERC Compliance Program issue and can not be addressed within individual standards.

Name	Company	Comments	Drafting Team Responses
Shelly Bell	San Diego Gas & Electric	<p>1. RE: NERC 1300 draft, section 1302  Comment: The risk-based assessment requirements discussed are not adequately defined. We'd like to see additional information such as acceptable criteria and methodology that should be used to determine critical bulk electric assets and critical cyber assets. Please provide documentation or a link to additional documentation to further explain this process.</p> <p>2. RE: NERC 1300 draft, section 1302 (a) 2 (i)  Comment: In this section, the definition of a critical cyber asset is discussed. When a cyber asset is identified as critical, the 1300 standard then applies to that asset (with all the various requirements that are described in 1300). Noticeably absent from this section is reference to the encryption of serial RTU communications between Master Station computers and field devices such as RTUs. The SDG&amp;E Grid Operations Cyber Team wishes to declare our support for the eventual inclusion of RTU serial data encryption, either in this standard, or in some future revision of 1300, when encryption hardware technology is more mature. We see this as a way to further increase the security and reliability of our Master Station -to- RTU communications channels.</p> <p>3. RE: NERC 1300 draft, section 1302 (a) 3  Comment: This section reads "A senior management official must approve the list of critical bulk electric assets and the list of critical cyber assets." The frequency of approval should be defined more precisely. We feel that this sort of approval is not practical on a frequent basis and would recommend a quarterly or bi-annual approval process.</p>	<p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p>

Name	Company	Comments	Drafting Team Responses
			<p>Specific to recommendations for modifying the previous 1302.g sections, the drafting team feels that the over-all re-drafting of 1302 has addressed this, particularly regarding the oversight responsibility for approving the respective lists of critical BES assets and critical cyber assets.</p> <p>Communications, at this time, is not included in the NERC cyber security standard.</p> <p>Senior management sign-offs are required at least annually. Senior management would not have to approve each change if a process was in place to ensure that changes to critical assets or cyber critical cyber assets are managed and documented within 30 days of the change.</p>
Stacy Bresler	PacifiCorp	1302.a".."preferred risk-based assessment" leaves room for poorly chosen assessment methodologies. Please define acceptable and unacceptable risk-assessment models or criteria. Additionally, how does NERC plan to determine what is/was preferred by the organization? Is it required that the preferred risk-based assessment methodology be documented?	Defining an acceptable risk-assessment model is outside the scope of the cyber security standard. The model documentation must include a description of the methodology including the determining criteria and evaluation procedure.



Name	Company	Comments	Drafting Team Responses
Terry Doern	BPA	<p>1302.a The term "critical bulk electric system asset" is first defined here, but not in the definitions section.</p> <p>The phrase "preferred risk-based assessment" should add the word "methodology" to the end.</p> <p>1302.a.2.i (B)(C)This is an alternate definition of critical cyber asset. A clearer definition is needed.</p> <p>Protocol and dial up are not measures of criticality, they are risks to the security of the asset.</p> <p>1302.a.3 BPA Transmission is in agreement with the WECC EMS WG's comment: Should be worded in a way that would enable identification by category, not just individual asset. Example would be that any device placed within the Energy Management System environment would automatically be covered and would not have to go to senior management.</p> <p>1302.g.3 As a federal agency, FISMA requires BPA to follow FIPS-199 as the standard by which to categorize the criticality all information and information systems.</p>	<p>The required definitons for the cyber security standard have been revised.</p> <p>The word "methodology" was not included as the responsible entity must use a process not necessarily a methodology.</p> <p>The standard does not preclude grouping of assets by category provided each asset is also listed.</p>

Name	Company	Comments	Drafting Team Responses
Tom Flowers	Centerpoint Energy	<p>Page 9, 1302 Critical Cyber Assets</p> <p>General comment:</p> <p>This section is ambiguous in several areas:</p> <p>(1)The language in 1302 and the FAQs associated with it seem to exclude the support systems and infrastructure at the control center, power plant, and substation such as UPS, batteries, computer room cooling systems, air handling systems, and switchgear for example. While these systems may not be critical infrastructure in another environment, the critical Cyber assets at the Control Center, Power Plant, and Substation are dependent on these systems to function normally."</p> <p>(2)Along these same lines, 1300 at this stage does not recognize the Remote Telemetry Unit (RTU) or other sensory/alarm devices at a critical substation as inherently being a critical Cyber asset even though the RTU may be the only source of situational awareness at that station for the Control Center critical Cyber assets. The standard, as written, defines the criticality of an RTU solely on its vulnerability instead of its role in the reliable operation of the bulk electric system. The RTU in the entity's most critical substation must also be the entities most critical RTU .</p> <p>(3)Nuclear Generation needs to be clearly excluded from this section.</p> <p>(4)There is no provision or discussion about one responsible entity declaring the assets of another responsible entity critical. What about one way dependencies?</p> <p>(5)There are several references to "common system" in this section. What does it mean (i.e. Region, Control Center, Plant Control System, etc.)?</p> <p>Specific Comments:</p> <p>Page 9, Introduction</p> <p>Replace the paragraph with... "The responsible entity shall identify and protect all critical Cyber assets related to the reliable operation of the bulk electric system."</p> <p>Page 9, (a)Requirements</p> <p>Replace the paragraph with.... " The responsible entity shall identify and inventory their critical bulk electric system assets using their preferred risk assessment methodology. All critical Cyber assets must be an identified subset of this inventory and protected in</p>	<ol style="list-style-type: none"> <li>1. The support systems and infrastructure at the control center, power plant, and substation such as UPS, batteries, computer room cooling systems, air handling systems, and switchgear are not covered by the cyber security standard.</li> <li>2. An RTU is covered by the cyber security standard if it meets the critical cyber asset criteria in section 1302.</li> <li>3. A reference to exclude nuclear facilities should be added to the standard.</li> <li>4. The responsible entity can use the "Additional Critical Asset" section to satisfy this requirement.</li> <li>5. For a common system the word "common" means "shared by or belonging to all".</li> </ol> <p>The section 1302 and required definitions have been re-written to address the above concerns.</p>

Name	Company	Comments	Drafting Team Responses
		<p>accordance with this Cyber security standard."</p> <p>Page 9, (a)(1)Critical Bulk Electric System Assets</p> <p>Replace the first two sentences with.... "The responsible entity shall identify its critical bulk electric system assets in accordance with the definition approved by the NERC Critical Infrastructure Protection Committee (see definitions)."</p> <p>Page 9, (a) (1)(ii)Critical Bulk Electric System Assets</p> <p>This subsection is ambiguous. Does this mean that any substation connected electrically to an element monitored for IROL purposes? If so, what substation doesn't?</p> <p>Page 9, (a) (1)(iii)Critical Bulk Electric System Assets</p> <p>Define "common system" or replace it.</p> <p>Page 9, (a) (1)(iv)Critical Bulk Electric System Assets</p> <p>Replace "initial" with "required for".</p> <p>Page 10, (a) (1)(v)Critical Bulk Electric System Assets</p> <p>Define "common system" or replace it.</p> <p>Page 10, (a) (2)Critical Cyber Assets</p> <p>This entire subsection needs to be reconsidered for technical content and scope. Here are several points that need to be addressed and clarified:</p> <ol style="list-style-type: none"> <li>1.Serial point-to-point (PTP) communication is not dial-up even though it may be over telephone lines</li> <li>2.RTUs (including PLS, smart meters, EIDs, etc) that supply critical situational awareness information to critical Cyber assets at the Control Center for critical Substations are inherently critical Cyber assets themselves regardless of their vulnerability.</li> <li>3.The support equipment (i.e. AC power, batteries, cooling, protective structure, etc.) that critical Cyber assets depend on to function are inherently critical Cyber assets because of this dependency.</li> </ol> <p>Pages 10 -12, (b) -- (f)</p> <p>CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.</p>	

Name	Company	Comments	Drafting Team Responses
Tom Pruitt	Duke Energy	<p>1302 There is confusion about which cyber assets are included in this section. Please clarify. This section seems to be more inclusive than that described in 1304. Why?</p> <p>Policy deviation documentation language is not left out of the standard as FAQ#4 indicates. What is the correct answer?</p> <p>What are the implications for dial-up language?</p> <p>1302(a)(2)(i) Are the protective relays which have dial in capability on an individual component level considered a critical cyber asset? Duke does not agree with the inclusion of individual protective relays.</p> <p>Please define use of the term "routable protocol." Specifically, is this limited to transport protocols (e.g., TCP/IP, UDP, etc.) or does it include application layer protocols such as DNP 3.0 serial or vendor proprietary protocols?</p> <p>Are cyber assets that are only accessible via point-to-point communications included or excluded with respect to this standard?</p> <p>1302(a)(2)(iii) What is the definition of "common system" as it is used here?</p> <p>1302(a)(3), pg 10 The term "officer" is used here and "official" is used other places. There is no reason to require an officer of the company to perform this role.</p> <p>Suggested re-wording: "This person, or his delegate (an approving authority), must authorize any deviation or exception from the requirements of this standard."</p> <p>Should be able to delegate approval. Suggested re-wording: "A senior management official, or their delegate (an approving authority), shall approve the list of critical bulk electric system assets and the list of critical cyber assets."</p> <p>1302(b) Should be labeled as "(b)" instead of "(g)." 1302 (a) is the requirements section. This is the next section.</p> <p>1302(b)(4)(i) Isn't this timeframe a little tight? For comparison, standard nuclear policies are much longer than 30 days for updating documentation.</p> <p>1302(b)(5), (i), &amp; (ii), pg 11</p> <p>Contains duplicate text, please delete duplication.</p> <p>The term "officer" is used here and "official" is used other places.</p>	<p>Issues with inconsistent outline sequencing and broken cross references are being addressed throughout the draft 1300 document.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those</p>

Name	Company	Comments	Drafting Team Responses
		<p>There is no reason to require an officer of the company to perform this role.</p> <p>1302(c) Should be "(c)" instead of "(h)"</p> <p>1302(d) Should be "(d)" instead of "(i)"</p>	<p>essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p> <p>Protective relays meeting the critical cyber asset criteria in section 1302 would be required to comply with the cyber security standard.</p> <p>"A senior management officer" should read "a member of senior management". Senior management sign-offs are required at least annually. Senior mangement would not have to approve each change if a process was in place to ensure that changes to critical assets or cyber critical cyber assets are manged and documented within 30 days of the change.</p>

Name	Company	Comments	Drafting Team Responses
Tony Eddleman	NPPD	<p>1302(a) - preferred risk-based assessment - what is this - a general, broad assessment or is it a specific format?</p> <p>1302(a)(1) - "significant impact on the ability to serve large quantities of customers for an extended period of time" What is considered "significant impact"? How many are "large quantities" - 10 or 10,000,000? How long is an "extended period of time" - 10 minutes or 10 months?</p> <p>1302(a)(1) - Define "a detrimental impact on the reliability or operability of the electric grid". Who determines a detrimental impact?</p> <p>1302(a)(1) - Define a "significant risk to public health and safety". Does this include every feeder that serves a traffic light, police station, hospital, senior care facility, jail, etc.? An argument could be made that this includes every line and substation in our system.</p> <p>1302(a)(1)(iv)(B) - Define "initial" system restoration. Are you referring to cranking paths for blackstart units to critical generation or enough of the system to get units stabilized or maybe something else?</p> <p>Recommend paragraph 1302(a)(2) Critical Cyber Assets be modified to specifically exclude all nuclear plants. These are covered under the Nuclear Regulatory Commission (NRC) standards.</p>	<p>Defining an acceptable risk-assessment model is outside the scope of the cyber security standard. The model documentation must include a description of the methodology including the determining criteria and evaluation procedure.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose a preferred risk-based assessment methodology for their environment.</p>

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.

A reference to exclude nuclear facilities should be added to the standard.

Name	Company	Comments	Drafting Team Responses
William Smith	Allegheny Energy	<p>2. 1302 -- Critical Cyber Assets</p> <p>The answer to FAQ 6 states that Critical Cyber Assets with dial-up access, which do not use a routable protocol, do not require the physical security perimeter requirements for critical cyber assets. Allegheny Energy believes that a routable protocol can also be secured in a sufficient manner to provide secure remote access. Therefore, Critical Cyber Assets located in substations with a sufficient local electronic security perimeter should not require the physical security perimeter requirements of critical cyber assets. Additionally, those attempting to compromise the physical security perimeter surrounding a critical cyber asset located within a substation would most likely have the ability to compromise the Critical Bulk Electric System Assets associated with the critical cyber asset first. The NERC guideline titled "Physical Security -- Substations" addresses substation security in sufficient detail.</p> <p>(a) Clarification is required on the selection of critical assets. The requirements begins by stating "that responsible entities shall identify their critical bulk electric system assets using their preferred risk-based assessment", then defines the bulk electric systems assets (differently than under the definitions), and then lists the bulk electric system assets.</p> <p>Does the listed bulk electric system assets serve as an overall view of "possible" bulk electric systems assets with each company able to subtract from this list based on their own risk-based assessment?</p> <p>(a)(2)(i)(A) Reword to "the cyber asset will cause an interruption or allow control of a critical bulk electric system asset, and"</p> <p>B)Reword to "the cyber asset uses a routable protocol for remote communications, or"</p> <p>D) Add "not" in between the words "do" and "use". Also, this item would be better suited in Section 1305 -- Physical Security and not in the definition section.</p>	<p>Cyber assets sharing an open (homogeneous) network environment -- i.e., inside the same electronic perimeter -- can put other critical cyber assets at risk and therefore must be protected equally. Even if the routable protocol is secured the critical cyber asset must be identified and secured according to all sections of the standard.</p> <p>The 1300 Drafting Team has given much consideration to numerous, and often conflicting, recommendations to modify the Preamble and other 1302 sections.</p> <p>The Preamble and previous 1302.a components have been re-drafted to reflect that the ability to identify those critical cyber assets that must be compliant with this standard is dependent on identifying the Bulk Electric System (BES) assets, functions, and tasks that are essential to maintaining reliable operation of the BES. Given 1300 will not further attempt to define BES, 1302 will only provide a minimum set of criteria for identifying those essential BES assets, functions, and tasks.</p> <p>1302 has been re-written to be clearer in its requirement that a formal, documented risk assessment process, based on the minimum criteria, be utilized to develop the list of essential BES assets, functions, and tasks. There are several risk assessment methodologies that are sufficient for this purpose. The goal is an accurate list of essential BES assets, functions, and tasks as a means of identifying critical cyber assets. The intent is not to track all BES assets, functions, and tasks. What is measured is that the list of essential BES assets, functions, and tasks exists, it is reviewed and updated routinely with over-sight sign-off, and that a documented formal process is in place to support this. The responsible entity is otherwise free to choose</p>



Name	Company	Comments	Drafting Team Responses
			<p>a preferred risk-based assessment methodology for their environment.</p> <p>Cyber assets that perform or otherwise support those essential assets, functions, and tasks, and that meet the minimum access criteria (re-drafted sections 1302.1.2 and 1302.1.3), are then identified as critical for purposes of this standard.</p>

# Comments on Section 1303 and Drafting Team Responses

Name	Company	Comments	Drafting Team Response
A. Ralph Rufrano	NYPA	<p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p>	<p>The Drafting Team will change the terminology to reflect Personnel Risk Assessment.</p> <p>Any personnel who have not been subject to Personnel Risk Assessment require supervised access or escort to critical cyber assets.</p> <p>Change made per input.</p> <p>Change made per input.</p> <p>The drafting team believes that a minimal level of background screening/risk assessment for all personnel is required..</p> <p>1302.a.2 will be changed as recommended.</p> <p>Will include reference to "documented company personnel risk assessment process".</p> <p>These items are implicit or addressed in Sections 1307 &amp; 1308.</p> <p>The standard will be reformatted.</p> <p>1303 Measures 4.i, includes contractors and service vendors.</p> <p>The drafting team believes that the requirement in 1303.Measures.4.i as currently drafted allows flexibility.</p> <p>1303. Measure 4.ii will be changed as recommended.</p> <p>1303.Measure.4.iii will be changed as recommended.</p> <p>1303.Measure.4.,iv, v and vi. Risk assessment terminology will be added. Identity verification will be changed to add flexibility for various country's laws based upon a number of similar comments. In light of</p>

Name	Company	Comments	Drafting Team Response
		<p>"Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p> <p>to</p> <p>"seven calendar days", per earlier comments and to keep consistent with FERC Order.</p> <p>1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments</p>	<p>other comments received these sections will be retained.</p> <p>Similar to other Human Resource records (e.g., employment applications, performance reviews, etc.), risk assessment documentation should be retained for duration of employment.</p> <p>Levels of non-compliance will be reviewed for consistency.</p> <p>1.ii changed.</p> <p>1.iii changed.</p> <p>1.iv will remain the same.3.iii changed.2.ii changed.</p> <p>1.v will remain the same.</p> <p>2.v changed.</p> <p>3.i will remain the same to address checks of third-party screening programs.</p> <p>3.ii changed.</p> <p>3.iv changed.</p> <p>Standard will be reformatted.</p>

Name	Company	Comments	Drafting Team Response
		<p>1303.Measure.4., remove; Subsections iv, v and vi.</p> <p>and replace with</p> <p>"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."</p> <p>1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".</p>	

Name	Company	Comments	Drafting Team Response
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Al Cooley	Verano	1303: Page 13, Section I, 2, iv, Personnel & Training: This section doesn't appear to make provision for the ideal case where preventive measures alert the entity to the fact that it is experiencing a cyber attack. Perhaps it could more effectively read: "Action plans and procedures to react to a detected or potential cyber incident, or to recover or re-establish critical cyber assets and access thereto following a cyber security incident."?	Incident detection, reporting, and recovery are addressed in other sections of the Standard.

Name	Company	Comments	Drafting Team Response
Allen Berman	LIPA	<p>1303 Personnel &amp; Training</p> <p>General Comment: Lettering of bullets must be corrected.</p> <p>(1) Measures</p> <p>(2) Training</p> <p>Comment: The Awareness section details periodic reinforcement of security requirements. However, the Training section does not detail any timeframes. Suggest that timeframes be associated with training.</p> <p>(1) Measures</p> <p>(4) Background Screening</p> <p>(ii)</p> <p>Comment: What constitutes "substantive change of personnel"?</p> <p>Comment: This section states that the list of personnel with access to critical cyber assets etc... will be updated within two business days of any substantive change of personnel. However, Section 1301 (b)(5)(i) requires that the list of individuals that authorize access to critical cyber information be updated within five days. These sections seem to contradict each other with respect to coordinating changes in personnel access and authorization.</p> <p>(1) Measures</p> <p>(4) Background Screening</p> <p>(iii)</p> <p>Comment: Suggest requiring that changes be made within 24 hours only for personnel who have had their access changed because of disciplinary action.</p>	<p>Standard will be reformatted.</p> <p>(1) Measures (2) Training</p> <p>Annual training added to training section.</p> <p>(1) Measures(4) Background Screening (ii)</p> <p>Substantive change of personnel includes transfers, resignations, suspensions, etc.</p> <p>Timeframes will be reviewed for consistency.</p> <p>(1) Measures (4) Background Screening (iii)</p> <p>Standard will be reviewed in light of comments received.</p>

Name	Company	Comments	Drafting Team Response
Charles Yeung	SPP	<p>1303 Personnel &amp; Training: Bullet resequencing needs to be consistent. Numbering goes from (a) Requirements to (l) Measures.</p> <p>1303 (l) (4) (ii) Background Screening: Requirement should read ". . . any substantive change of personnel or substantive change in responsibility of authorized personnel."</p> <p>1303 (l) (4) (iv) Background Screening: The Social Security Number verification is a USA-only requirement. The SSN equivalent in Canada is precluded by Canadian law from being used in this context.</p>	<p>Standard will be reformatted.</p> <p>1303 (l) (4) (ii) Background Screening Too prescriptive. Can be adopted by responsible entities, as required.</p> <p>1303 (l) (4) (iv) Background Screening More flexibility for applicable laws will be addressed.</p>



<b>Name</b>	<b>Company</b>	<b>Comments</b>	<b>Drafting Team Response</b>
Charlie Salamone	NSTAR	1303a.4 - Unrestricted access needs clarification. Should this be unescorted?	1303a.4 wlll be changed to authorized.

Name	Company	Comments	Drafting Team Response
Chris DeGraffenied	NYPA	<p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p> <p>"Background Screening: All personnel having access to critical cyber assets,</p>	See Responses to A. Ralph Rufano

Name	Company	Comments	Drafting Team Response
		<p>including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p> <p>to</p> <p>"seven calendar days", per earlier comments and to keep consistent with FERC Order.</p> <p>1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments</p> <p>1303.Measure.4., remove;</p>	

Name	Company	Comments	Drafting Team Response
		<p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."</p> <p>1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assessment program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assessment program exists, but is not consistently applied, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assessment program does not exist, or"</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to</p>	

Name	Company	Comments	Drafting Team Response
		"personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Dave McCoy	Great Plains Energy	<p>1303 - Under Measures under Records it is stated that the responsible entity shall maintain documentation that it has reviewed its training program annually. Shouldn't this say review and update. It would seem that this mandate should also include the updating of cyber security training programs.</p> <p>1303 There are multiple references to the time frame for implementing access changes. (See list of references below.) It would be helpful if the requirements were stated clearly and centralized in one place:</p> <p>1303 (l) Measures (4) Background Screening (iii) Access revocation must be completed within 24 hours for any personnel who have a change in status where they are not allowed access to critical cyber assets</p> <p>1303 (l) Measures (4) Background Screening (ii) update the listing [of personnel with access to critical cyber assets] within two business days of any substantive change of personnel.</p> <p>1303 (o) Levels of Noncompliance (1) Level One (ii) instance of personnel termination (employee, contractor or service provider) in which the access control list was not updated within 2 business days</p>	<p>The requirement for reviewing and updating will be added.</p> <p>Timeframes will be reviewed for consistency</p>

Name	Company	Comments	Drafting Team Response
David Kiguel	Hydro One	<p>While we agree with the intent of Section 1303, the use of the term "background screening" however has too many issues and we recommend that this section's title become "Personnel Risk Assessment." Portions of 1303 are too prescriptive and our position is that that the responsible entity should have more latitude in determining what is an acceptable level of risk. We have made recommendations later in the comment form that will make this Section acceptable.</p> <p>1303: Hydro One agrees with the intent of Section 1303. However, the term "background screening" has too many issues and we recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>On background screening, "Social Security Number (SSN)" is a unique identification number used strictly in the United States. The Canadian equivalent to it is "Social Insurance Number (SIN)". However, Canadian law prescribes SIN to be used specifically for income tax purposes only, and for nothing else. Hence, the use of SSN or SIN in the standard is inappropriate. We recommend the re-phrasing of Section 1303, b, (4), (iv) as: "The responsible entity shall conduct background screening of all personnel prior to being granted access to critical cyber assets. A minimum of an appropriate identity verification and a criminal check with a seven year retrospective scope are required. Entities may conduct more detailed reviews depending upon the criticality of the position. Update screening shall be conducted at least every five years, or for cause. These requirements are subject to all applicable laws, and to existing collective bargaining unit agreements. "</p> <p>Hydro One supports the notion of applying for a waiver, in case the entities fail to reach an agreement on background checks with bargaining units. However, at the same, we support providing a proof of efforts by the entities to reach agreements in the next contract negotiation.</p> <p>Additionally, Canadian entities are tightly constrained as to any forms of drug testing. Hence, CEA member would have difficulty supporting any move in the current and future standards to include drug testing, except for just cause.</p>	<p>The Drafting Team will change the terminology to reflect Personnel Risk Assessment.</p> <p>1303 (l) (4) (iv) Background Screening More flexibility for applicable laws will be addressed.</p> <p>Drug screening will not be specified as a requirement in this standard, although it will not specifically preclude the possibility of applicable entities' establishing more stringent criteria should they wish.</p> <p>See responses to A. Ralph Rufrano.</p>

Name	Company	Comments	Drafting Team Response
		<p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>The FAQ describes "supervised access." However 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>In 1303 Measures.2, add a training measure section for disaster recovery (1308) and incident response planning (1307).</p> <p>1303.Compliance Monitoring Process.2, we do not agree with "background screening documents for the duration of employee employment." Change the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.a.2 from</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets."</p> <p>In 1303.Measures.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days otherwise", per earlier comments</p> <p>Remove iv, v and vi. Replace with "There must be a documented company personnel risk assessment process."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven</p>	



Name	Company	Comments	Drafting Team Response
		<p>days otherwise" (as mentioned earlier). Change "personnel termination" to "personnel change in access status."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, requires clarification. Does this measure include third party personnel?</p> <p>Change 1303.Measures.4.i from</p> <p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s).</p> <p>to</p> <p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s).</p> <p>In 1303.Measures.4.ii, change from "two business days" to "seven calendar days", as per earlier comments.</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assessment program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-</p>	

Name	Company	Comments	Drafting Team Response
		Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303. Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the identation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
David Little	Nova Scotia Power	<p>We agree with the intent of Section 1303. The term - background screening- however has too many issues, we recommend that this section's title become - Personnel Risk Assessment. Portions of 1303 are too prescriptive, the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic. Change 1303.a.4 from -unrestricted access- to -authorized access. Change 1303.a.4 title to -Personnel Risk Assessment. Change 1303.a.4 to -A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks.</p> <p>Change 1303.a.2 from;  Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets.  to  The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets</p> <p>1303.a.4 from;  (4) Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets.  to  (4) Personnel Risk Assessment: There must be a documented company personnel risk assessment process.</p> <p>Add to 1303 Measures.2, a training measure section for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s).</p> <p>to</p> <p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s). )."</p> <p>(there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from</p> <p>two business days</p> <p>to</p> <p>seven calendar days, per earlier comments and keep consistent with FERC Order.</p> <p>1303.Measure.4.iii, change -24 hours- to -24 hours if terminated with cause or disciplinary action, or seven days-, per earlier comments</p> <p>1303.Measure.4., remove;</p> <p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities.</p> <p>1303.Compliance Monitoring Process.2, We do not agree with - background screening documents for the duration of employee employment. and suggest changing the last bullet in (i) to - Verification that Personnel Risk Assessment is conducted.</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change 24 hours to be consistent with earlier comments. Change personnel termination to personnel change in access status .</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of Background investigation program exists, but consistent selection criteria</p>	

Name	Company	Comments	Drafting Team Response
		is not applied, or to Personnel risk assement program is practiced, but not properly documented, or	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to Personnel risk assement program exists, but is not consistently applied, or	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to Personnel risk assement program does not exist, or	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status .	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to Access control list exists, but is incomplete.	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from cover two of the specified items to cover two or more of the specified items.	
		Correct the identation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Deborah Linke	US Bureau of Reclamation	<p>(2) Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and the protection of sensitive information about or within these critical assets. - The authors may want to consider specifically addressing incident response and contingency operations training for appropriate individuals.</p> <p>(4) Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets.- The authors may want to consider escort requirements for service vendors and visitors who do not have appropriate background investigations. Obviously, it is impractical for all access to be unrestricted. This requirement could impact costs associated with janitorial/custodial services as well as that provided by some vendors.</p> <p>(iii) Access revocation must be completed within 24 hours for any personnel who have a change in status where they are not allowed access to critical cyber assets (e.g., termination, suspension, transfer, requiring escorted access, etc.). - This time should probably be shorter than this if the termination or suspension is an adverse action and the critical cyber system allows access from outside the organization.</p> <p>(iv) The responsible entity shall conduct background screening of all personnel prior to being granted access to critical cyber assets in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements. A minimum of Social Security Number verification and seven year criminal check is required. Entities may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position. - What actions are suggested for incumbents who may be found to not meet background screening minimum criteria, but whose employment has been satisfactory?</p>	<p>Training issues are dealt with in Sections 1307 and 1308.</p> <p>This background screening issue is addressed in the FAQs for Section 1303.</p> <p>(4) Background Screening (iii) Industry comments received in response to 1300 do not support this opinion. However, the 24-hour requirement does not preclude applicable entities' establishing shorter timeframes should they wish. As a practical matter, many companies do.</p> <p>(4) Background Screening (iv) Guidance is contained in the publication referenced in the FAQ's.</p>

Name	Company	Comments	Drafting Team Response
Dennis Kalma	AESO	<p>1303.a.4 We would like to see some guidance in the FAQ about how to handle any negative results from a background check especially suggested tolerance levels.</p> <p>We find it unusual that with this level of scrutiny, the standard has not addressed random drug and alcohol testing of serving employees.</p> <p>1303.a.4 (1) 4 (1v) For Canada – Social Insurance Number (SIN)</p>	<p>1303.a.4 Guidance is contained in the publication referenced in the FAQ's.</p> <p>Drug screening will not be specified as a requirement in this standard because of the diversity in applicable laws and related issues. The standard does not, however, preclude the possibility of applicable entities' establishing more stringent criteria should they wish.</p> <p>1303.a.4 (1) 4 (1v) The standard will be updated.</p>

Name	Company	Comments	Drafting Team Response
Doug Van Slyke	ATCO Electric	<p>Section 1303 - Personnel &amp; Training It is not reasonable to have to do a seven year criminal check on all employees who are granted access to critical cyber assets. The requirement to conduct this screening on all personnel every five years seems a bit drastic as well. Checking on vendors and contractors is understandable but not on employees unless they are a new employee to the company. What if this infringes on current privacy laws? Maybe more understanding of intent would help here.</p>	<p>Section 1303 - Personnel &amp; Training  The standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p>



Name	Company	Comments	Drafting Team Response
Ed Goff	Progress Energy	<p>1303 Personnel &amp; Training</p> <p>- b.4.ii - b.4.iii - Background Screening &amp; Access -- These sections tend to blur Background Screening requirements and action required for access control updates. Access control should be broken out separately and consider NERC previous final comment to the 1200 urgent action standard, NERC conceded that 24 hours may not be practical and suggested an alternative stating: - that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence. In the case of contractor/vendor employees, they shall be required to promptly advise the system owner/operator when such changes occur and system access should be updated as soon as practical but no later than three business days after notification. This requirement looks to be right out of the nuclear world...concerned that this will have the same level of overhead as our nuclear facilities. We are uncertain about the costs associated with this requirement but feel it will be significant.</p> <p>- b.4.ii Background screening [page 14] - any substantive change - What exactly is meant by 'substantive'? This is too vague and has too much room for interpretation.</p>	<p>1303 Personnel &amp; Training</p> <p>- b.4.ii - b.4.iii</p> <p>This section has been changed to reflect within 24 hours for cause terminations and 7 calendar days for other personnel actions.</p> <p>- b.4.ii Substantive changes include transfers, resignations, suspensions, etc.</p>

Name	Company	Comments	Drafting Team Response
Ed Riley	CAISO	<p>1303.a.1 Replace "personnel subject to the standard " to "personnel having access to critical cyber assets".</p> <p>1303.a.4 Where background screening may be a deterrent, it can cause a false sense of security. By only performing "common" corporate background screenings, someone the is fraudulently acting as someone else is normally not detected. Only more through background screening like fingerprinting can provide the necessary assurance that someone is who they say they are.</p> <p>Also, this does not account for non-US citizens. A lot of our workforce is working with green cards and background screening would not provide any value for this scenario.</p> <p>Using "escorted access" and "unescorted access" is better terminology than "unrestricted access".</p> <p>1303.L.4.iii Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.</p>	<p>1303.a.1 Not accepted. There could be critical cyber assets outside the scope of the standard.</p> <p>1303.a.4 Applicable entities are not precluded from establishing striciter crteria, based upon individual needs. The standard sets minimums.</p> <p>Foreign nationals can be screened via various means, including through 3rd party providers, who can provide advice in this area.</p> <p>Unrestricted access will be changed to authorized access.</p> <p>1303.L.4.iii Timelines have been adjusted for consistency.</p> <p>References to SSN and SIN have been eliminated in favor of identity verification.</p>

Name	Company	Comments	Drafting Team Response
Ed Stein	FirstEnergy	<p>1303 (ii) (page 14) states The Responsible entity shall review the document (list of access) and update listing with in 2 days of a 'substantive change' of personnel. No definition of 'substantive change' was provided.</p> <p>1303 Personnel &amp; Training</p> <p>Page 13 "Awareness Program: Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate Awareness section be deleted.</p> <p>Page 14 Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: Responsible entities shall ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status.</li> <li>- 1303 (ii) (page 14) states The Responsible entity shall review the document (list of access) and update listing with in 2 days of a 'substantive change' of personnel. No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states Access revocation must be completed with 24 hours for personnel who are not allowed access (e.g. termination, suspension, transfer, requiring escorted access, etc.). This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations 24 hours.</li> </ul> <p>Regarding requirements for updating access records, ABC recommends:</p> <ol style="list-style-type: none"> <li>1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat Routine administrative changes should be handled within three</li> </ol>	<p>1303 ii Substantive changes include transfers, resignations, suspensions, etc.</p> <p>1303 Personnel &amp; Training Awareness is the on-going reinforcement of good security practices, while training is generally time-bound and periodic, so awareness supports the training efforts.</p> <p>Access Changes: The standard will be modified to reflect within 24 hours for personnel terminated for cause and 7 business days for other personnel changes.</p> <p>Background Screening: Reference to SSN and SIN have been eliminated in favor of identity verification.</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p> <p>A higher level of background screening identifies the need for a higher standard of trust for employees having access to critical cyber assets. If existing program comply, they would be acceptable under the standard.</p> <p>Records: Applicable entities are not expected to disclose results of background screens, but must demonstrate that screening has been done for relevant personnel. The stanard does not dictate that these records be kept within a specific organizational department.</p> <p>Unrestricted has been changed to authorized access. It is the individual entity who determines the degree of authorized access to provide its contractors and services vendors.</p> <p>Timeframes will be changed to a minimum of 24 hours</p>

Name	Company	Comments	Drafting Team Response
		<p>business days after occurrence.</p> <p>2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</p> <p>3. If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.</p> <p>Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:  - "...A minimum of Social Security Number verification..."  Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.</p> <p>NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "...organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.</p> <p>ABC recommends one of the following to replace proposed Standard 1300 language:  A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.  Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.  Requiring the screening of all personnel every 5 years should be deleted.  B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be</p>	<p>for personnel terminated for cause and 7 calendar days for other personnel changes.</p>

Name	Company	Comments	Drafting Team Response
		<p>documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.</p> <p>Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.</p> <p>Page 13: Records: " ...background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.</p> <p>Page 15 (i) Standard 1300 language implies that background check lists &amp; verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.</p> <p>Page 13: Background screening: Proposed language states: "...contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?</p> <p>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</p>	

Name	Company	Comments	Drafting Team Response
Ernst Everett	OGE	Section 1303 - Need to do away with background screening on a five year interval and require updates for cause only. Only the latest background investigation results need be kept.	The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.

Name	Company	Comments	Drafting Team Response
Francis Bradley	CEA	<p>On background screening, "The Social Security Number (SSN)" is a unique identification number used strictly in the United States. The closest Canadian equivalent is the "Social Insurance Number (SIN)". However, Canadian law strictly limits the uses to which the SIN number can be put, and for this reason it is inappropriate for the Standard to prescribe the use of SIN numbers for background checking.. CEA recommends the re-phrasing of Section 1303, b, (4), (iv) as: "The responsible entity shall conduct background screening of all personnel prior to being granted access to critical cyber assets. A minimum of an appropriate identity verification and a criminal check with a seven year retrospective</p>	<p>References to SSN and SIN have been eliminated in favor of identity verification.</p>

Name	Company	Comments	Drafting Team Response
Francis Flynn	National Grid	<p>National Grid agrees with the intent of Section 1303. The term "background screening" however has too many issues for the National Grid and recommends that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and National Grid feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations in the Question 3 Section response of this form that will make this Section acceptable.</p> <p>1303, National Grid agrees with the intent of Section 1303. The term "background screening" however has too many issues for National Grid and recommends that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and National Grid feels that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic. Change 1303.a.4 from "unrestricted access" to "authorized access". Change 1303.a.4 title to "Personnel Risk Assessment." Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p>	Please see responses to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Response
		1303.a.4 from;	
		"(4) Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."	
		to	
		"(4) Personnel Risk Assessment: There must be a documented company personnel risk assessment process."	
		Add to 1303 Measures.2, a training measure section for disaster recovery (1308) and incident response planning (1307).	
		The numbering of 1303 starting with Measures needs correction.	
		1303 Measures 4.i, request clarification. Does this include third party personnel?	
		Change 1303.Measures.4.i from;	
		"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."	
		to	
		"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)."	
		Change 1303.Measures.4.ii from;	
		"two business days"	
		to	
		"seven calendar days", per earlier comments and keep consistent with FERC Order 2004b.	
		1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments	

Name	Company	Comments	Drafting Team Response
		<p>1303.Measure.4., remove;</p> <p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>"There must be a documented company personnel risk assessment process." National Grid feels these subsections are too prescriptive. Additionally, references to Social Security Numbers do not apply to Canadian entities.</p> <p>1303.Compliance Monitoring Process.2, National Grid does not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, Change "Background investigation program exists, but consistent selection criteria is not applied, or"</p> <p>to</p> <p>"Personnel risk assement program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist,</p>	

Name	Company	Comments	Drafting Team Response
		or"	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours for cause or.. , or. seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours for cause or.., or seven days for all.." (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the identification for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Gary Campbell		<p>1303</p> <p>This requirement again has requirements imbedded within the measures. I believe the "requirements" set the minimum, the "measures" tell me what to go and look for and "levels of compliance" tell me the degree of severity for not having the minimum requirements met.</p> <p>Levels of compliance;</p> <p>Level 1 I do not think checking for consistent selection criteria is a function of reliability compliance. Wouldn't it be a human resource issue?</p> <p>Please define key personnel? Define applied consistently?</p> <p>Level 2 iii - Are we referring to specific items in requirements? iv - if any Awareness program does not exist how can it be implemented?</p> <p>Level 3 iii - I would think this item should be quite severe. I suggest moving to level 4</p>	<p>Level 1 non-compliance suggests a collaboration between the applicable responsible entity and whatever resources are required for compliance within member companies (e.g., Human Resources, Security, Legal, etc.).</p> <p>Key personnel are those subject to this standard. Consistently is defined as a demonstrated on-going reinforcement of security awareness.</p> <p>Level 2 iii addresses the requirements.</p> <p>The drafting does not agree that the this item should be moved.</p>

Name	Company	Comments	Drafting Team Response
Guy Zito	NPCC	<p>NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p> <p>"Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p>	

Name	Company	Comments	Drafting Team Response
		to	
		"seven calendar days", per earlier comments and to keep consistent with FERC Order.	
		1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments	
		1303.Measure.4., remove;	
		Subsections iv, v and vi.	
		and replace with	
		"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."	
		1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-	

Name	Company	Comments	Drafting Team Response
		Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	



Name	Company	Comments	Drafting Team Response
Hein Gerber	British Columbia Transmission Corp	<p>1303 Personnel and Training Under Canadian laws the use of Social Insurance Number (equivalent to US Social Security Number) is voluntary and cannot be enforced. The standard should provide for the use of appropriate alternate identities in Canada.</p> <p>1303 Personnel and Training Compliance monitoring as described paragraph (n) section (2) should be expanded to include contractors and service vendors for the duration of their contracts or service agreements.</p>	<p>References to SSN and SIN have been eliminated in favor of identity verification.</p> <p>1303 Personnel and Training Compliance monitoring as described paragraph (n) section (2) will be expanded to include contractors and service vendors for the duration of their contracts or service agreements.</p>

Name	Company	Comments	Drafting Team Response
Howard Ruff	WE Energies	<p>Section 1303, Personnel and Training</p> <p>We question the requirement to provide all individuals who have access to critical cyber assets to undergo the same levels of awareness and security training. Those individuals who have logical access to critical cyber assets should undergo more rigorous training around cyber security and awareness than those who only have access to the physical location where the cyber assets reside (example: janitorial staff). Strongly recommend that individuals with unescorted access to critical cyber assets on the day the revised requirements become effective should be granted continuing access (grandfathered) without the need for a background investigation. No periodic re-investigation should be required.</p>	<p>Individual entities can structure the training &amp; awareness to meet their defined needs. The Standard sets the minimum requirements.</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p>

Name	Company	Comments	Drafting Team Response
Jeff Schlect	Avista Corporation	Background checks -- For a number of administrative burden and liability risk issues, it is requested that existing employees of the organization be exempted from this requirement. Any background check requirement should be applicable for new employees to the organization only.	The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.

Name	Company	Comments	Drafting Team Response
Jim Hiebert	WECC EMS WG	<p>1301.a.1 Replace "personnel subject to the standard " to "personnel having access to critical cyber assets".</p> <p>1303.I.4.iii Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.</p>	<p>There may be critical cyber assets outside the scope of the standard.</p> <p>The standard will be reviewed for consistency.</p> <p>References to SSN and SIN have been eliminated in favor of identity verification.</p>

Name	Company	Comments	Drafting Team Response
Joanne Borrell	First Energy Services	<p>1303 Personnel &amp; Training</p> <p>Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.</p> <p>Page 14 Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>Regarding requirements for updating access records, ABC recommends:</p> <ol style="list-style-type: none"> <li>1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</li> <li>2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>3. If the item is used to identify non-compliance, all references</li> </ol>	Please see response to Ed Stein.

Name	Company	Comments	Drafting Team Response
		throughout the document should reflect the revised requirements.	
		<p>Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:</p> <p>- "...A minimum of Social Security Number verification..."</p> <p>Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.</p>	
		<p>NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "...organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.</p>	
		<p>ABC recommends one of the following to replace proposed Standard 1300 language:</p> <p>A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.</p> <p>Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.</p> <p>Requiring the screening of all personnel every 5 years should be deleted.</p> <p>B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.</p>	

Name	Company	Comments	Drafting Team Response
		<p>Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.</p>	
		<p>Page 13: Records: " ...background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.</p>	
		<p>Page 15 (i) Standard 1300 language implies that background check lists &amp; verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.</p>	
		<p>Page 13: Background screening: Proposed language states: "...contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?</p>	

Name	Company	Comments	Drafting Team Response
John Blazeovitch	Exelon	<p>1303.a.4 This sentence reads: unrestricted access to critical assets. We recommend that the sentence read: unrestricted access to critical cyber assets. Please define the term unrestricted access</p> <p>1303.1.4.iii This section requires access revocations within 24 hours of a change in status. We agree that access must be updated within 24 hours for cases where a person loses his/her access rights due to cause. The NRC allows three days for a favorable termination and this standard should not be more demanding than the highly regulated nuclear industry. We believe that routine administrative status changes should be managed within six business days.</p> <p>The scope of access revocation is not clear. We recommend that the sentence begin: Physical and electronic access revocation</p> <p>1303.1.4.iv 1303.a.4 requires that personnel shall be subject to background screening prior to being granted unrestricted access to critical [cyber] assets. We recommend that the first sentence of 1303.1.4.iv read: The responsible entity shall conduct background screening of all personnel prior to being granted unrestricted access...</p> <p>1303.1.4.vi This section requires that background screening be conducted at least every five years, or for cause. Since employees of the responsible entity are under constant observation by management personnel and performance is reviewed on an on-going basis, we believe that it is not necessary to renew the background investigation for employees.</p>	<p>1303.a.4 Unrestricted access will be changed to authorized access.</p> <p>1303.1.4.iii The standard will be changed to reflect within 24 hours for termination for cause and 7 calendar days for other personnel changes.</p> <p>Access revocation will be clarified as physical and electronic access revocation.</p> <p>1303.1.4.iv Unrestricted access will be changed to authorized access.</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p>



Name	Company	Comments	Drafting Team Response
John Hobbick	Consumers Energy	1303 Personnel and Training 1) Awareness & 2) Training Awareness on a quarterly basis will be very burdensome to accomplish. Annual training/refreshers is all that is required and the Awareness section should be dropped.	Awareness can be accomplished through a variety of techniques (see FAQs) and should not be overly burdensome.

Name	Company	Comments	Drafting Team Response
John Lim	ConEd	<p>In section 1303, in the background screening requirement, clarify what "unrestricted access" means. The FAQ should clarify whether THIS standard should require background screening for system operators using the control application or just personnel with "unrestricted access" ( both physical or logical) with the ability to damage or otherwise compromise the critical cyber asset hardware, software, data or network component.</p> <p>Also in this section, the requirement to revoke access within 24 hours is too restrictive. Section 1301 allows 5 days for updating access records for changes. We suggest 24 hours only for terminations for cause, and 7 days for all other cases of status changes, and that these be consistently applied in all sections where access updates are required.</p>	<p>Unrestricted will be changed to authorized.</p> <p>The standard will be changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p>

Name	Company	Comments	Drafting Team Response
Karl Tammer	ISO-RTO Council	<p>1303.a Using "escorted access" and "unescorted access" is better terminology than "unrestricted access" and is a better terminology to reinforce and enforce.</p> <p>1303.I.4 The ISOs/RTOs have a number of regional concerns related to national, state, provincial, and local laws and requirements. These concerns will be submitted individually.</p> <p>1303.O.ii: This needs to align more closely with the previous benchmark of "24 hours" and escalate based on this bench mark.</p>	<p>1303.a The standard will be modified to use the term authorized access.</p> <p>1303.O.ii: has been changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p>

Name	Company	Comments	Drafting Team Response
Kathleen Goodman	ISO-NE	<p>1303 Preamble: The 1300 standard must be very clear in that it does not mandate what department within a responsible entity is accountable for security training and/or background screening, and related records management.</p> <p>1303 Requirements: Remove the word "unrestricted." It is possible to grant unsupervised access with some restrictions.</p> <p>(2) Training: Include disaster recovery (re; 1308.a.4) as training requirement</p> <p>(4) Background Screening (4.i) through (4.ii) these have nothing to do with performing background screening – Remove. (4.iii) What does this have to do with conducting/documenting background screening? Otherwise, see previous 1301.Requirements.5.iv -- 24-hour requirement is unrealistic in most cases. Requirement should be within 24 hours for facility and remote access for terminations with cause or other disciplinary action. Next Business Day for all other access. (4.iv) through (vi) which is attempts to legislate employment practices and is too overreaching -- e.g., it states that we must discipline consistently and comport with our collective bargaining agreements. These are not appropriate subjects for a NERC standard. Likewise for the specifics on background checks, which are sensitive and subject to various laws (including the Fair Credit Reporting Act). We prefer not to see potentially conflicting standards established here.</p> <p>1303 Levels Noncompliance (1.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from? This needs to align more closely with the previous benchmark of "24 hours" and escalate based on this benchmark.</p> <p>(2.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from?</p> <p>(3.ii) - ...access control list was not updated within 2 business days - completely different requirement - where did 2 business days come from?</p>	<p>The standard does not mandate specific departmental responsibilities.</p> <p>Unrestricted will be replaced with authorized. Training is addressed in Section 1308.</p> <p>(4) Background Screening (4.i) through (4.ii) This list provides the information necessary to determine the personnel who will be subject to background screening.</p> <p>(4.iii)The standard will be changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p> <p>(4.iv) through (vi) The drafting team believes these requirements accommodate the diversity in law. See FAQs.</p> <p>1303 Levels Noncompliance(1.ii),(2.ii),(3.ii) The standard will be changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p>

Name	Company	Comments	Drafting Team Response
Ken Goldsmith	Alliant Energy	<p>1303 Personnel and Training</p> <p>Within this section, personnel, employees and contractors are used interchangeably and it is not clear when contractors are included or not included.</p> <p>Article 1-1 Security awareness reinforcement is important but for the standard to dictate and measure quarterly seems excessive. Suggest it state periodic security awareness reinforcement with a focus on annual training of the NERC standard.</p> <p>Article 1-4-i, ii, and iii The first three paragraphs under background screening are covered elsewhere in the standard. Suggest removing from this section.</p> <p>Article 1-4-v The standard should not address adverse employment.</p> <p>Article 1-4-vi Requiring background investigations every 5 years for existing employees should occur for performance reasons only. Background investigations for existing employees should be dependent on corporate policy.</p> <p>Article n-2-i Change Reviews to Security Awareness.</p>	<p>Anyone having access to critical cyber assets, as defined by the Standard, are included, whether employees or 3rd parties.</p> <p>Article 1-1 Awareness can be accomplished through a variety of techniques and should not be overly burdensome.</p> <p>Article 1-4-i, ii, and iii These sections support the documentation required for effective administration of the screening program.</p> <p>Article 1-4-v The standard addresses consistency and adherence to accepted legal practices, not specific actions.</p> <p>Article 1-4-vi The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p> <p>Reviews will be changed to Security Awareness.</p>

Name	Company	Comments	Drafting Team Response
Larry Brown	EEI Security Committee	<p>Section 1303</p> <p>(a)(4) The term "unrestricted access" does not appear anywhere else – delete, or (even better) clarify and use consistently (i.e., some access may be restricted and thus may not require as high a level of employee/contractor clearance).</p> <p>At an appropriate location, add subsection (b)(2) from Section 1306, as that is more appropriate for this section (revise and renumber format).</p> <p>(l)(1) &amp; (l)(2) It should be made more clear that only "Awareness," and not formal "Training," is required quarterly.</p> <p>(l)(4)(iii) The stipulation of 24 hours is too short for all except dismissals "for cause" (see earlier comments above). Routine transfers, retirements, etc., should have at least three days, ideally five, and perhaps even seven, as determined by the utility to be appropriate and consistent with other corporate policy.</p> <p>Check formatting and revise/correct as necessary.</p> <p>(l)(4)(iv) Clarify that the minimum check is required "if and only if" there is unrestricted access (see comment above on [a][4]).</p> <p>Check formatting and revise/correct as necessary.</p> <p>(n)(2)(i)(4th bullet) What is meant by the term "reviews"? Its meaning is not clear from the context alone.</p> <p>Check formatting and revise/correct as necessary.</p> <p>(o)(3)(v), (vi), &amp; (vii)– The subparagraphs should be renumbered – such as: (o)(4), (4)(i), and (4)(ii) and in general check formatting and revise/correct as necessary.</p>	<p>The term unrestricted access will be changed to authorized access.</p> <p>The drafting team believes password management should remain in Section 1306.</p> <p>Clarification will be added to (l)(1) &amp; (l)(2).</p> <p>(l)(4)(iii) The standard will be changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p> <p>(l)(4)(iv) Changed to reflect “authorized” access</p> <p>(n)(2)(i)(4th bullet) Reveiws will be changed to “security awareness”.</p> <p>The standard will be reformatted.</p>

Name	Company	Comments	Drafting Team Response
Larry Conrad	Cinergy	<p>1303– Personnel &amp; Training</p> <p>Page 13 "Awareness Program: Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. Cinergy recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.</p> <p>Page 14 Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are. -1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status." -1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided. -1303 (iii) (page 14) states Access revocation must be completed with 24 hours for personnel who are not allowed access (e.g. termination, suspension, transfer, requiring escorted access, etc.). This implies the time requirement may be different for other changes. -1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</p> <p>Regarding requirements for updating access records, Cinergy recommends:</p> <ol style="list-style-type: none"> <li>1.The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</li> <li>2.The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>3.If the item is used to identify non-compliance, all references</li> </ol>	Please see responses provided to Ed Stein, First Energy

Name	Company	Comments	Drafting Team Response
		<p>throughout the document should reflect the revised requirements.</p> <p>Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:  - "...A minimum of Social Security Number verification..."  Language as written will deny access to anyone except U.S. citizens. Cinergy recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.</p> <p>NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "...organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." Cinergy again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.</p> <p>Cinergy recommends one of the following to replace proposed Standard 1300 language:  A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.  Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.  Requiring the screening of all personnel every 5 years should be deleted.  B. If the above proposed language is not acceptable as an alternative by NERC, then Cinergy recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.</p> <p>Page 13: Language states that a "higher level of background</p>	



Name	Company	Comments	Drafting Team Response
		<p>screening" should be conducted on personnel with access. Cinergy's background screening for new hires complies with the NERC requirements and other legal requirements. Cinergy does not agree that multiple levels of background screening are required. Cinergy recommends that the reference to multiple levels of background screening be deleted.</p> <p>Page 13: Records: " ...background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." Cinergy does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.</p> <p>Page 15 (i) Standard 1300 language implies that background check lists &amp; verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at Cinergy.</p> <p>Page 13: Background screening: Proposed language states: "...contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?</p>	

Name	Company	Comments	Drafting Team Response
Laurent Webber	WAPA	<p>Reference 1303, Personnel and Training (1)(2)(iv) - Training on recovery of critical cyber assets should be tied to the system or structure (Under NIST this is part of the Security Plan) and not general Cyber Security Awareness training. This comment also applies to 1308 Recovery Plans (a)(4).</p> <p>Section 1303, Measures (4)(iv), is one of many examples of too much proscriptive detail. All the background screening criteria should be altered/simplified to only say that a utility must have a policy related to the screening and must follow that policy and be able to show the records that the policy was followed.</p> <p>Section 1303, Requirement (4), the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1303, Measure (4)(iv).</p> <p>Section 1303, under Requirements (1). It appears the phrase, "Responsible entity shall comply with the following requirements of this standard," should precede items 1 through 4, not be part of item 1.</p>	<p>(1)(2)(iv) Left to company discretion. Requirement reflected in 1303 is a minimal requirement. 1308 changed to reflect consistency with 1303.</p> <p>Section 1303, Measures (4)(iv) establishes minimum requirements and entities are free to implement more stringent review, if warranted. Many member companies without existing screening programs have asked from more, not less, guidance on how these programs should be conducted, and that is addressed in the FAQ's for this section.</p> <p>Section 1303, Requirement (4), the term unrestricted access will be changed to authorized access.</p> <p>Requirements (1) will be revised as suggested.</p>

Name	Company	Comments	Drafting Team Response
Linda Campbell	FRCC	<p>1303 Personnel &amp; Training</p> <p>Many of the measures within this section appear to be more like requirements than measures. For example, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening could be the measure. We would suggest a thorough review of this section.</p> <p>Another example - The requirements and compliance sections indicate that records shall be kept on background screening, but the measures states records shall be kept for training.</p> <p>It is unrealistic to track, do background screening, and train all personnel who ever walk by critical cyber assets. We recommend the following changes:</p> <p>First paragraph – change "personnel having access" to personnel having "unescorted or unsupervised access"</p> <p>(a) This section should require a list of "personnel with access" be implemented and maintained.</p> <p>(a)(1) "Awareness" should be placed under 1303(a)(2) Training.</p> <p>(a) (2) Training – Change "All personnel having access to critical..." to "All personnel having unescorted or unsupervised access to critical"</p> <p>(a) (3) Records – Change "of all personnel having access to critical..." to "of all personnel having unescorted or unsupervised access to critical.. "</p> <p>(a)(3) "Records" should be placed under 1303(a)(2) Training.</p> <p>(a) (4) Suggest changing wording from All personnel with access to critical cyber....being granted unrestricted access...." to "All personnel having unescorted or unsupervised access to critical cyber..... being granted unrestricted access"</p> <p>(a) (4) Background Screening</p> <p>The requirement for background screening will become particularly onerous and costly for many organizations. For example, in some areas of a generating station it is not possible to establish a discrete physical security perimeter around every critical cyber asset. During periods of construction/maintenance at a generating station, hundreds of contract laborers may be present and the requirement to</p>	

Name	Company	Comments	Drafting Team Response
		background screen these personnel would significantly impact the cost and time required to complete construction efforts. How should an organization address this issue and stay in compliance with the standard?	
		Note on the related FAQ - The FAQ for this section seems to be out of synch with the numbering in the standard.	
		(l) Measures (think this should have been (b) )	
		(l) (2) – Training should be given based on the roles assigned to individuals not one-size- fits-all training for all personnel. For instance, not all personnel with access to cyber assets require training in recovery plans for cyber assets.	
		(l) (3) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"	
		(l) (4) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"	
		(l) (4) (ii) Background Screening- reference to 1303.2.4.1 – section doesn't exist. "Substantive change" is an un-defined term	
		(l) (4) (iii) Background Screening It is unclear why measures (i, ii, iii) for the personnel list, update of the list, and access revocation is covered under background screening. Is this stating that access must only be removed for anyone whose change in status occurs as a result of the background screening? If this is not the case, we believe that 24 hours (note non-compliance states 2 days) is an unreasonable expectation for access revocation, except in the case where the individual represents a potential threat to the organization. In most large organizations transfers, changes in responsibilities and routine employee separation cannot be communicated to personnel responsible for physical and cyber access management within this timeframe, not to mention situations where the personnel may work for a 3rd party contracting firm. We recommend that at least 3 business days be allowed for routine personnel movement access changes.	
		(l) (4) (iv) Suggest changing "being granted access" to "being granted unescorted or unsupervised access" it is not reasonable to have	

Name	Company	Comments	Drafting Team Response
		background checks on every vendor ever in a computer room. Social security number verification should not be a requirement as it eliminates foreign nationals.	
		(l) (4) (v) The Q&A indicates that "adverse employment actions" are related to the background screening, but this is not apparent in the way it is worded. Suggest making it more clear. Perhaps "adverse employment actions resulting from background screening results"....	
		(l) (4) (vi) This requirement for update screening of personnel every 5 years is onerous and extremely costly. In addition, it indicates lack of trust of our valued long term employees and should be removed or changed to indicate criteria should be established within the background screening procedures for what might trigger the need for an update screening.	
		(m) – (p) is mis "numbered" – should be (c), (d), etc. references in (n) (2) don't exists	
		(n) (2) The requirement exists to keep records on the background screening for the duration of employee employment. Does this mean the responsible entity must keep records on background screening for both employees and contract personnel? The FAQ indicates that the responsible entity must only ensure that background screening is performed for those third parties, in which case the responsible entity would not have those records. There appears to be inconsistency here. Many of our vendors have already indicated they will perform background checks, but will not provide records about their employees to us.	
		(n) (2) (i) bullet 3 – what checklist are you referring to??	
		(o) (1) (iii) – Should say Background "screening" not "investigation". (also in (o) (2) (v))	
		"Consistent selection criteria is not applied" – what is this referring to? Selection criteria is not mentioned in the requirements or the measures.	
		(o)(3)(i) States 2 business days when 1303(l)(4)(iii) measurement states 24 hours.	
		(o)(3)(ii) Though this violation refers to the Access Revocation of Section 1303(l)(4)(iii), it is really a duplication of Section 1301(a)(5)(iv). The Noncompliance of Section 1301(a)(5)(iv) is	

Name	Company	Comments	Drafting Team Response
		<p>stated as not being accomplished within 24 hours [Section 1301(e)(4)(xi)]. The incongruity of these two sections should be rectified.</p>	

Name	Company	Comments	Drafting Team Response
Lloyd Linke	WAPA - MAPP	<p>Section 1303, under Measures (4) (iv) is one of many examples of too much proscriptive detail. At least one entity in MAPP is not allowed to do criminal back-ground checks with local law enforcement, and so requiring that be done for the last seven years is not acceptable. The background screening criteria should all be altered/simplified to only say that a utility must have a policy related to the screening, and must follow that policy and be able to show the records that it was followed.</p> <p>Section 1303, Requirement (4) the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1303, Measure (4) (iv)</p> <p>Section 1303, under Requirements (1). It appears like the phrase "Responsible entity shall comply with the following requirements of this standard" should precede items 1 through 4, not be part of item 1..</p>	Please see response to Laurent Webber.

Name	Company	Comments	Drafting Team Response
Lyman Schaeffer	Pacific Gas & Electric	<p>1303 Personnel and Training</p> <p>The language in the proposed standard is far superior to that currently in place in the emergency action standard. We generally concur with the requirement to provide security related training as well as a requirement for background investigations for new employees, contractors, or other third parties who have unsupervised access to critical cyber assets. However, we strongly question the need to perform background investigations on an ongoing basis for existing employees. In general, these are individuals who have been employed by the company for some period of time and who have already gone through background screening as part of their initial employment. Moreover, unlike the majority of third parties or contractors, they are subject to constant observation as to their behavior and fitness by company supervisory and management personnel. The usefulness of a background investigation escapes us since it is highly unlikely to detect a potential terrorist.</p> <p>We note that the standard appropriately leaves the actual implementation of adverse actions against an employee to the individual utility and subject to collective bargaining agreements. However, the end result is that this standard, if implemented, will cause considerable animosity between companies and employees with little real enhancement of the security of the enterprise. We believe that the better alternative is to have each company establish a procedure for identifying individuals who have demonstrated unreliability based on documented behavior as well as the mechanisms to deal with that behavior.</p> <p>We also strongly dispute the need to remove employees from access lists within the timeframes described in the standard. We believe a better measure is to require that those persons whose access is removed due to termination, suspension, or some other behavior related cause should be removed within 24 hours. However, routine transfers, retirements, and other normal personnel actions should require removal within five working days or more.</p> <p>We also believe that requiring formal training on cyber security matters on a quarterly basis is excessive and will eventually undermine its effectiveness. We believe that a training requirement for a single comprehensive annual session providing training on the cyber security requirements with a less intensive refresher training session is sufficient.</p>	<p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p> <p>The timeframes for changing access lists have been changed to 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p> <p>The standard requires quarterly security awareness reinforcement, which can be accomplished through a variety of techniques (see FAQs).</p>



Name	Company	Comments	Drafting Team Response
Michael Allgeier	LCRA	1303 Personnel Security DHS, RCMP and Intel. databases need to be included in the initial background check. i.e. the terrorist watch lists.	Section 1303 defines the minimum requirement. It does not not preclude entities establishing more stringent background screening criteria, such as the use of DHS, RCMP, and other sources of information.

Name	Company	Comments	Drafting Team Response
Michael Anderson	Midwest ISO	<p>Background Checks – Can a recommendation be made on how to handle the background screenings for contractors with critical system access? Is it enough to have a trusted relationship with the vendor and utilize their background screen information for their employees or must each individual contractor employee be screened by the individual company?</p> <p>Training Requirements – Can the requirement for training of personnel with access to critical systems assets be made clearer? The document implies that employees with access to critical cyber assets be held to a different standard and receive a different set of training.</p>	<p>Screening by the Contractor/service vendor is acceptable, as long as it meets the intent of 1303 and is verified by the responsible entity.</p> <p>All personnel having access to critical cyber assets must have the training specified in section (b)(2) “Training”.</p>

Name	Company	Comments	Drafting Team Response
Neil Phinney	Georgia Transmission Co	1303.a.4 Background screening is required only for people being given unrestricted access to critical assets. This implies that if access is limited in any way, a background check would not be required.	Unrestricted will be changed to authorized.

Name	Company	Comments	Drafting Team Response
Paul McClay	Tampa Electric Company	<p>1303 Personnel &amp; Training</p> <p>Many of the measures within this section appear to be more like requirements than measures. For example, lists of personnel with access are not mentioned in the requirements, but appear in the measures. Periodic background screening would be a requirement, and having documentation of such background screening could be the measure. We would suggest a thorough review of this section.</p> <p>Another example - The requirements and compliance sections indicate that records shall be kept on background screening, but the measures states records shall be kept for training.</p> <p>It is unrealistic to track, do background screening, and train all personnel who ever walk by critical cyber assets. We recommend the following changes:</p> <p>First paragraph – change "personnel having access" to personnel having "unescorted or unsupervised access"</p> <p>(a) (2) Training – Change "All personnel having access to critical..." to "All personnel having unescorted or unsupervised access to critical"</p> <p>(a) (3) Records – Change "of all personnel having access to critical..." to "of all personnel having unescorted or unsupervised access to critical.. "</p> <p>(a) (4) Suggest changing wording from All personnel with access to critical cyber....being granted unrestricted access...." to "All personnel having unescorted or unsupervised access to critical cyber..... being granted unrestricted access"</p> <p>(a) (4) Background Screening</p> <p>The requirement for background screening will become particularly onerous and costly for many organizations. For example, in some areas of a generating station it is not possible to establish a discrete physical security perimeter around every critical cyber asset. During periods of construction/maintenance at a generating station, hundreds of contract laborers may be present and the requirement to background screen these personnel would significantly impact the cost and time required to complete construction efforts. How should an organization address this issue and stay in compliance with the standard?</p> <p>Note on the related FAQ - The FAQ for this section seems to be out of synch with the numbering in the standard.</p>	<p>1303 Personnel &amp; Training</p> <p>The standard will be reviewed for clarity and consistency.</p> <p>The term authorized access will be used.</p> <p>(a) (4) Background Screening</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's. Contractors conducting routine work at power plants, etc., would generally be physically restricted from critical assets (see physical security section) or escorted when provided access to those assets, and not all would be required to be screened under the Standard.</p> <p>(a) (2), (a) (3), and (a) (4) The term unescorted will be changed to authorized.</p> <p>(l) (2) Specialized training is at the discretion of individual entities.</p> <p>(l) (3) (i) , (l) (4) (i) The drafting team does not agree with these suggestions.</p> <p>(l) (4) (ii) Substantive changes include transfers, resignations, suspensions, etc.</p> <p>(l) (4) (iii) Access revocation requirements will be changed to reflect within 24 hours for termination for cause, and 7 calendar days for other personnel actions.</p> <p>(l) (4) (iv) The standard will be changed to reflect "authorized" access, and SSN/SIN requirement will be changed to "identity verification".</p> <p>(l) (4) (v) The wording will be reviewed for clarity.</p> <p>(l) (4) (vi) See response above.</p>

Name	Company	Comments	Drafting Team Response
		<p>(l) Measures (think this should have been (b) )</p> <p>(l) (2) – Training should be given based on the roles assigned to individuals not one-size- fits-all training for all personnel. For instance, not all personnel with access to cyber assets require training in recovery plans for cyber assets.</p> <p>(l) (3) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"</p> <p>(l) (4) (i) Suggest changing wording from "all personnel with access to critical cyber" to "all personnel having unescorted or unsupervised access to critical cyber"</p> <p>(l) (4) (ii) Background Screening- reference to 1303.2.4.1 – section doesn't exist. "Substantive change" is an un-defined term</p> <p>(l) (4) (iii) Background Screening It is unclear why measures (i, ii, iii) for the personnel list, update of the list, and access revocation is covered under background screening. Is this stating that access must only be removed for anyone whose change in status occurs as a result of the background screening? If this is not the case, we believe that 24 hours (note non-compliance states 2 days) is an unreasonable expectation for access revocation, except in the case where the individual represents a potential threat to the organization. In most large organizations transfers, changes in responsibilities and routine employee separation cannot be communicated to personnel responsible for physical and cyber access management within this timeframe, not to mention situations where the personnel may work for a 3rd party contracting firm. We recommend that at least 3 business days be allowed for routine personnel movement access changes.</p> <p>(l) (4) (iv) Suggest changing "being granted access" to "being granted unescorted or unsupervised access" it is not reasonable to have background checks on every vendor ever in a computer room. Social security number verification should not be a requirement as it eliminates foreign nationals.</p> <p>(l) (4) (v) The Q&amp;A indicates that "adverse employment actions" are related to the background screening, but this is not apparent in the way it is worded. Suggest making it more clear. Perhaps "adverse</p>	<p>The standard will be reformatted and references corrected.</p> <p>That is acceptable. The responsible entity is only required to validate the contractor program.</p> <p>(n) (2) (i) bullet 3 It is used as an example of the type of records entities may maintain for compliance.</p> <p>(o) (1) (iii), (o) (2) (v))The standard will be reviewed for consistency. Consistent criteria should applied to the selection/retention of personnel per accepted industry standards, as referenced in the FAQ's</p>

Name	Company	Comments	Drafting Team Response
		<p>employment actions resulting from background screening results"....</p> <p>(l) (4) (vi) This requirement for update screening of personnel every 5 years is onerous and extremely costly. In addition, it indicates lack of trust of our valued long term employees and should be removed or changed to indicate criteria should be established within the background screening procedures for what might trigger the need for an update screening.</p> <p>(m) – (p) is mis "numbered" – should be (c), (d), etc. references in (n) (2) don't exists</p> <p>(n) (2) The requirement exists to keep records on the background screening for the duration of employee employment. Does this mean the responsible entity must keep records on background screening for both employees and contract personnel? The FAQ indicates that the responsible entity must only ensure that background screening is performed for those third parties, in which case the responsible entity would not have those records. There appears to be inconsistency here. Many of our vendors have already indicated they will perform background checks, but will not provide records about their employees to us.</p> <p>(n) (2) (i) bullet 3 – what checklist are you referring to??</p> <p>(o) (1) (iii) – Should say Background "screening" not "investigation". (also in (o) (2) (v)) and "Consistent selection criteria is not applied" – what is this referring to? Selection criteria is not mentioned in the requirements or the measures.</p>	

Name	Company	Comments	Drafting Team Response
Pedro Modia	FPL	<p>Change on at least quarterly" to "annually" under Measures (l)(1).</p> <p>Change 1303 (4)(iii) to add for cause.</p> <p>Further clarification is required in regards to "investigations upon complaint". How intrusive are these investigations, and what would predicate such investigations?</p>	<p>This change was made.</p> <p>The standard will be changed to reflect minimum of 24 hours for personnel terminated for cause and 7 calendar days for other personnel actions.</p> <p>The terminology is “investigation for cause” and would only be a last resort for reviewing program failures outside the normal compliance review process.</p>

Name	Company	Comments	Drafting Team Response
Pete Henderson	IMO	<p>1303 Personnel &amp; Training</p> <p>(a) Requirements (4) Background Screening</p> <p>The wording of this requirement should be consistent with 1303 (1) (4) (iv): viz: "All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets in accordance with federal, state, provincial, and local laws, and subject to applicable collective bargaining unit agreements.</p> <p>(I) Measures (4) - Background Screening</p> <p>In subsection (vi) it is adequate to specify that updated screening should be done for cause. Periodic re-screening (every 5 years) is not required as good management practice includes observing changes in employee behaviour and circumstance that would prompt further investigation as necessary.</p> <p>Subsection (iv) The Social Security Number (SSN)" is a unique identification number used strictly in the United States. The closest Canadian equivalent is the "Social Insurance Number (SIN)". However, Canadian law strictly limits the uses to which the SIN number can be put, and for this reason it is inappropriate for the standard to prescribe the use of SIN numbers for background checking.</p> <p>(n) Compliance Monitoring Process (2)</p> <p>The phrase, "where not prohibited by law or applicable collective bargaining agreements" should be added to the phrase, "Document(s) for compliance, training, awareness, and screening".</p> <p>(o) Levels of Noncompliance</p> <p>(1) Level One</p> <p>Nowhere in the Requirements portion of 1303 is there a reference to "consistent selection criteria", so subsection (o) (1) (iii) should not be a measure of non-compliance.</p> <p>(3) Level Three</p> <p>1303 (o) (3) (iv) should be 1303 (o) (4).</p>	<p>(a) Requirements (4) Background Screening</p> <p>Requirements set the high-level tone, while the measures provide the detail.</p> <p>(I) Measures (4) - Background Screening</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's. Contractors conducting routine work at power plants, etc., would generally be physically restricted from critical assets (see physical security section) or escorted when provided access to those assets, and not all would be required to be screened under the Standard.</p> <p>Subsection (iv)</p> <p>(n) Compliance Monitoring Process (2)</p> <p>Record keeping is generally not subject to law or collective bargaining agreements.</p> <p>(o) Levels of Noncompliance</p> <p>Consistent criteria should applied to the selection/retention of personnel per accepted industry standards, as referenced in the FAQ's</p>



Name	Company	Comments	Drafting Team Response
Phil Sobol	SPP CIPWG	The Requirements section of 1303 states that background checking is required for those being granted "unrestricted access to critical assets"? What about those who have restricted access? The Measures section of 1303 makes no distinction.	Unrestricted has been changed to “authorized”

Name	Company	Comments	Drafting Team Response
Ray A'Brial	CHGE	<p>CHGE's participating members agrees with the intent of Section 1303. The term background screening however has too many issues for CHGE participating members and recommend that this section's title become Personnel Risk Assessment. Portions of 1303 are too prescriptive and CHGE's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>1303, CHGE's participating members agrees with the intent of Section 1303. The term background screening however has too many issues for the CHGE participating members and recommend that this section's title become Personnel Risk Assessment. Portions of 1303 are too prescriptive and CHGE's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>(a)(4) – Term unrestricted access does not appear anywhere else – delete, or (even better) clarify and use consistently (i.e., some access may be restricted and thus may not require as high a level of employee/contractor clearance).</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 title to Personnel Risk Assessment.</p> <p>Change 1303.a.4 to A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks.</p> <p>Change 1303.a.2 from;</p> <p>Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets.</p> <p>to</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets</p>	
		1303.a.4 from;	
		<p>Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets.</p>	
		to	
		<p>Personnel Risk Assessment: There must be a documented company personnel risk assessment process.</p>	
		<p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p>	
		The numbering of 1303 starting with Measures needs correction.	
		<p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p>	
		Change 1303.Measures.4.i from;	
		<p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s).</p>	
		to	
		<p>Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s). (CHGE believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p>	

Name	Company	Comments	Drafting Team Response
		<p>Change 1303.Measures.4.ii from;</p> <p>two business days</p> <p>to</p> <p>seven calendar days, per earlier comments and to keep consistent with FERC Order.</p> <p>1303.Measure.4.iii, change 24 hours to 24 hours if terminated with cause or disciplinary action, or seven days, per earlier comments</p> <p>1303.Measure.4., remove;</p> <p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>There must be a documented company personnel risk assessment process. these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities</p> <p>1303.Compliance Monitoring Process.2,</p> <p>(i)(4th bullet) What is meant by reviews?</p> <p>CHGE's participating members do not agree with background screening documents for the duration of employee employment. and suggest changing the last bullet in (i) to Verification that Personnel Risk Assessment is conducted.</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of Background investigation program exists, but consistent selection criteria is not applied, or" to Personnel risk assement program is practiced, but not properly documented, or</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-</p>	

Name	Company	Comments	Drafting Team Response
		Compliance.1.v to Level Two	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to Personnel risk assement program exists, but is not consistently applied, or	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to Personnel risk assement program does not exist, or	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to Access control list exists, but is incomplete.	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from two days to 24 hours with cause or seven days (as mentioned earlier). Change personnel termination to personnel change in access status.	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from cover two of the specified items to cover two or more of the specified items.	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Ray Morella	First Energy	<p>1303 – Personnel &amp; Training</p> <p>Page 13 "Awareness Program": Once again, this section contains requirements without any documented evidence that such requirements will enhance security. Requiring both training program and awareness program seems redundant and burdensome. ABC recommends that the awareness in inherent in training and is part of the training requirements. We recommend that the separate "Awareness" section be deleted.</p> <p>Page 14 Access Changes: By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1301 &amp; 1306) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are. - 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status." - 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided. - 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes. - 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</p> <p>Regarding requirements for updating access records, ABC recommends:</p> <ol style="list-style-type: none"> <li>1. The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</li> <li>2. The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>3. If the item is used to identify non-compliance, all references</li> </ol>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Response
		throughout the document should reflect the revised requirements.	
		<p>Page 14: Background Screening. The entire section on background screening, as written in Standard 1300, is problematic. For example:</p> <p>- "...A minimum of Social Security Number verification..."</p> <p>Language as written will deny access to anyone except U.S. citizens. ABC recommends that the language requiring a social security number be deleted unless it is NERC's intent that only U.S. citizens and no one else is granted electronic or physical access.</p>	
		<p>NERC showed insight when, in their Responses to comments submitted during the balloting of the Urgent Action Cyber Security Standard 1200, NERC wrote: "...organizations are NOT required to conduct background investigations of existing employees given the fact that they have had the opportunity to observe and evaluate the behavior and work performance of those employees after they have been employed for a period of time." ABC again recognizes that Standard 1300 is a different standard from Standard 1200; however, the logic that provided the foundation for the previous NERC comment is sound. If the company has had an opportunity to observe the long service employee, the background screen requirement should be relaxed.</p>	
		<p>ABC recommends one of the following to replace proposed Standard 1300 language:</p> <p>A. The requirement should include background screening for all individuals (employees and vendors) who seek approval for new permanent access to critical cyber assets.</p> <p>Background screening on existing employees, previously approved for access, is appropriate if there is cause to suspect the individual of suspicious behavior.</p> <p>Requiring the screening of all personnel every 5 years should be deleted.</p> <p>B. If the above proposed language is not acceptable as an alternative by NERC, then ABC recommends language be inserted indicating that background screening requirements will be evaluated by the company involved, and the policy toward such screenings will be documented by that company. Company will be free to document policies such as: At Company's discretion, long service employees, which the Company has observed, may be grandfathered and background checks will not be done on these employees. Company will not be found in non-compliance for such a policy.</p>	

Name	Company	Comments	Drafting Team Response
		<p>Page 13: Language states that a "higher level of background screening" should be conducted on personnel with access. ABC's background screening for new hires complies with the NERC requirements and other legal requirements. ABC does not agree that multiple levels of background screening are required. ABC recommends that the reference to multiple levels of background screening be deleted.</p>	
		<p>Page 13: Records: " ...background screening of all personnel having access to critical cyber assets shall be provided for authorized inspection upon request." ABC does not agree that the background screen information obtained on all its employees will be provided to NERC inspectors. In the 10/18 Webcast NERC stated that it is not their intent that the contents of the background screening be provided to the inspectors. Recommendation: Improve language so that it is clear that contents of background screen need not be divulged to inspectors.</p>	
		<p>Page 15 (i) Standard 1300 language implies that background check lists &amp; verifications are kept by operations groups responsible for the cyber security implementation. Such records will continue to be maintained by the Human Resource Department at ABC.</p>	
		<p>Page 13: Background screening: Proposed language states: "...contractors and service vendors, shall be subject to background screen prior to being granted unrestricted access to critical assets." Is it NERC's intention that they be granted unrestricted access after completing a background screen as stated in 1300?</p>	



Name	Company	Comments	Drafting Team Response
Richard Engelbrech	Rochester Gas & Electric	<p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p> <p>"Background Screening: All personnel having access to critical cyber assets,</p>	Please see response to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p> <p>to</p> <p>"seven calendar days", per earlier comments and to keep consistent with FERC Order.</p> <p>1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments</p> <p>1303.Measure.4., remove;</p>	

Name	Company	Comments	Drafting Team Response
		<p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."</p> <p>1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to</p>	

Name	Company	Comments	Drafting Team Response
		"personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Richard Kafka	PEPCO	<p>Definition: Define Having Access for the purpose of Section 1303? [Is this only for physical access?]</p> <p>Definition (Section 1303.a.4): The term Unrestricted Access does not appear anywhere else. Please clarify meaning and use (i.e. some access may be restricted and thus may require different levels of employee/contractor clearance).</p> <p>Definition (Section 1303.n.2.i.4th bullet): What is meant by Reviews?</p>	<p>Applies to both physical and cyber access.</p> <p>1303.a.4: Unrestricted will be changed to authorized.</p> <p>Section 1303.n.2.i. Reviews will be changed to Security Awareness</p>

Name	Company	Comments	Drafting Team Response
Robert Pelligrini	United Illuminating	<p>NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This</p>	Please see response to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p> <p>"Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p>	

Name	Company	Comments	Drafting Team Response
		to	
		"seven calendar days", per earlier comments and to keep consistent with FERC Order.	
		1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments	
		1303.Measure.4., remove;	
		Subsections iv, v and vi.	
		and replace with	
		"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."	
		1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-	



Name	Company	Comments	Drafting Team Response
		Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Robert Strauss	NYSEG	<p>NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>1303, NPCC's participating members agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NPCC participating members and recommend that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and NPCC's participating members feel that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic.</p> <p>Change 1303.a.4 from "unrestricted access" to "authorized access".</p> <p>Change 1303.a.4 title to "Personnel Risk Assessment."</p> <p>Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This</p>	Please see response to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Response
		<p>program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p> <p>1303.a.4 from;</p> <p>"Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."</p> <p>to</p> <p>"Personnel Risk Assessment: There must be a documented company personnel risk assessment process."</p> <p>Add to 1303 Measures.2, a training measures for disaster recovery (1308) and incident response planning (1307).</p> <p>The numbering of 1303 starting with Measures needs correction.</p> <p>1303 Measures 4.i, request clarification. Does this include third party personnel?</p> <p>Change 1303.Measures.4.i from;</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."</p> <p>to</p> <p>"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)." (NPCC believes there may be instances that require differing levels of access to various perimeters in different locations of varying importance.)</p> <p>Change 1303.Measures.4.ii from;</p> <p>"two business days"</p>	

Name	Company	Comments	Drafting Team Response
		to	
		"seven calendar days", per earlier comments and to keep consistent with FERC Order.	
		1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments	
		1303.Measure.4., remove;	
		Subsections iv, v and vi.	
		and replace with	
		"There must be a documented company personnel risk assessment process." NPCC's participating members feel these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."	
		1303.Compliance Monitoring Process.2, NPCC's participating members do not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"	
		Move 1303.Compliance Monitoring Process.Levels of Non-	

Name	Company	Comments	Drafting Team Response
		Compliance.1.iv to Level Three	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".	
		Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."	
		Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii	

Name	Company	Comments	Drafting Team Response
Roman Carter	Southern Company	<p>1303 (Personnel and Training)</p> <ul style="list-style-type: none"> <li>• In the measures section (l)(4)(ii), we need a definition of a 'substantive' change of personnel. Also the document should be reviewed at a minimum annually.</li> <li>• In (n)(1), does that process belong in the standard definition since compliance is a regional matter? Is it not more appropriate in the regional compliance enforcement plan?</li> <li>• 1303(l)(4)(iii) is not referenced in any way in the "Levels of Noncompliance" for 1303. If it does not impact the compliance level, then its not enforceable and thus not needed in the Measures</li> <li>• 1303(o)(1)(i) "... not been updated or reviewed for more than three months but less than six months; ..." This has the practical effect of requiring reviews more frequently than quarterly because reviews take a finite period of time. In other words if one waits exactly 3 months to perform the review it will be in violation if it takes any time to perform the review. If the review takes place earlier than 3 months (e.g. 2.5 months) it still must do the next one faster than 3 months from the previous review, thus resulting in more frequent than 4 times a year review. If the intent is to review quarterly, either some grace period is needed to complete the review, such as "has not been updated or reviewed for more than four months but less than six months" or the words "per calendar quarter" or something similar need to be used.</li> <li>• (o)(3)(v) This should be 1303(o)(4).</li> <li>• (o)(3)(vi)-(vii) should be re-sequenced 1303(o)(4)(i)-(ii).</li> <li>• (a)(4) Add – Restricted physical or electronic access may be granted to contractors or service vendors by authorized escorts or active monitoring of access.</li> <li>• (l)(1) Security awareness reinforcement should be done on an annual as opposed to quarterly basis. • (l)(2) Training programs should be conducted annually as opposed to quarterly.</li> <li>• (l)(4)(iv) A drug screen and national criminal history check should be included in the required minimum. • (l)(4)(v) Add – "for ensuring the trustworthiness and reliability of personnel with physical or electronic access.</li> <li>• (l)(4)(vi) Delete "at least every five years".</li> <li>• (n)(1)(4th bullet) Delete "quarterly and annual" and insert "as required".</li> <li>• (n)(1)(5th bullet) Add - "and any corrective adverse action based on background checks is being conducted".</li> <li>• (o)(1)(i) Change to "list of personnel is available but has not been reviewed within one year:.</li> <li>• (o)(1)(v) Change to "Awareness program exists but not applied</li> </ul>	<p>(l)(4)(ii) Further defined in the following section (iii).</p> <p>(n)(1) This just reinforces the overall process.</p> <p>1303(l)(4)(iii) If it does not impact the compliance level, then its not enforceable and thus not needed in the Measures It is referenced in the Levels of Compliance in 3 sections.</p> <p>1303(o)(1)(i) Changes are required upon all relevant personnel as indicted in section (n)(4)(iii), and the Compliance Monitoring language addresses delinquencies in making those changes as defined in section 1303.</p> <p>(o)(3)(v) Formatting will be addressed in the next revision.</p> <p>(a)(4) Unrestricted changed to authorized.</p> <p>(l)(1) Security awareness can be conducted with a variety of media, as suggested in 1303, and should not be onerous.</p> <p>(l)(2) Clarified to be annual training.</p> <p>(l)(4) Individual companies can employ measures beyond the minimums specified. Drug screening has numerous challenges in Canada and various states.</p> <p>(l)(4)(v) Suggetion is redundant to existing language.</p> <p>(l)(4)(vi) The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p> <p>(n)(1)(4th bullet and 5th bullet) The drafting team does not agree.</p> <p>(o)(1)(i) The drafting team disagrees.</p> <p>(o)(1)(v) The drafting team believes this is too prescriptive.</p> <p>(o)(1)(ii) Changed to 24 hours for personnel terminations for cause and 7 calendar days for other personnel actions.</p>

Name	Company	Comments	Drafting Team Response
		<p>consistently or with the minimum of annual reinforcement)".</p> <ul style="list-style-type: none"> <li>• (o)(1)(ii) Change to " ..not updated within 5 business days".</li> </ul>	

Name	Company	Comments	Drafting Team Response
S. Kennedy Fell	NYISO	<p>The NYISO agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NYISO and recommends that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and the NYISO feels that the responsible entity should have more latitude in determining what is an acceptable level of risk and have made recommendations later in the form that will make this Section acceptable.</p> <p>1303, The NYISO agrees with the intent of Section 1303. The term "background screening" however has too many issues for the NYISO and recommends that this section's title become "Personnel Risk Assessment". Portions of 1303 are too prescriptive and the NYISO feels that the responsible entity should have more latitude in determining what is an acceptable level of risk.</p> <p>The FAQ describes supervised access, 1303 does not touch upon this topic. Change 1303.a.4 from "unrestricted access" to "authorized access". Change 1303.a.4 title to "Personnel Risk Assessment." Change 1303.a.4 to "A risk assessment process will be in place that determines the degree of supervision required of personnel with access to critical cyber assets. This process will incorporate assessment of misconduct likelihood which could include background checks."</p> <p>Change 1303.a.2 from;</p> <p>"Training: All personnel having access to critical cyber assets shall be trained in the policies, access controls, and procedures governing access to, the use of, and sensitive information surrounding these critical assets."</p> <p>to</p> <p>"The responsible entity shall develop and maintain a company-specific cyber security training program that will be reviewed annually. This program will insure that all personnel having access to critical cyber assets will be trained in the policies, access controls, and procedures governing access to, and sensitive information surrounding these critical cyber assets"</p>	Please see response to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Response
		1303.a.4 from;	
		"(4) Background Screening: All personnel having access to critical cyber assets, including contractors and service vendors, shall be subject to background screening prior to being granted unrestricted access to critical assets."	
		to	
		"(4) Personnel Risk Assessment: There must be a documented company personnel risk assessment process."	
		Add to 1303 Measures.2, a training measure section for disaster recovery (1308) and incident response planning (1307).	
		The numbering of 1303 starting with Measures needs correction.	
		1303 Measures 4.i, request clarification. Does this include third party personnel?	
		Change 1303.Measures.4.i from;	
		"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the security perimeter(s)."	
		to	
		"Maintain a list of all personnel with access to critical cyber assets, including their specific electronic and physical access rights to critical cyber assets within the respective security perimeter(s)."	
		Change 1303.Measures.4.ii from;	
		"two business days"	
		to	
		"seven calendar days", per earlier comments and keep consistent with FERC Order.	
		1303.Measure.4.iii, change "24 hours" to "24 hours if terminated with cause or disciplinary action, or seven days", per earlier comments	

Name	Company	Comments	Drafting Team Response
		<p>1303.Measure.4., remove;</p> <p>Subsections iv, v and vi.</p> <p>and replace with</p> <p>"There must be a documented company personnel risk assessment process." The NYISO feels these subsections are too prescriptive and also references to Social Security Numbers do not apply to Canadian entities."</p> <p>1303.Compliance Monitoring Process.2, The NYISO does not agree with "background screening documents for the duration of employee employment." and suggest changing the last bullet in (i) to "Verification that Personnel Risk Assessment is conducted."</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.ii, change "24 hours" to be consistent with earlier comments. Change "personnel termination" to "personnel change in access status".</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iii, instead of "Background investigation program exists, but consistent selection criteria is not applied, or" to "Personnel risk assement program is practiced, but not properly documented, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.v to Level Two</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.v to "Personnel risk assement program exists, but is not consistently applied, or"</p> <p>Move 1303.Compliance Monitoring Process.Levels of Non-Compliance.1.iv to Level Three</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iii to "Personnel risk assement program does not exist, or"</p> <p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.2.ii from "two days" to "24 hours with cause or seven</p>	

Name	Company	Comments	Drafting Team Response
		<p>days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".</p>	
		<p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.i to "Access control list exists, but is incomplete."</p>	
		<p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.ii from "two days" to "24 hours with cause or seven days" (as mentioned earlier). Change "personnel termination" to "personnel change in access status".</p>	
		<p>Change 1303.Compliance Monitoring Process.Levels of Non-Compliance.3.iv from "cover two of the specified items" to "cover two or more of the specified items."</p>	
		<p>Correct the indentation for 1303.Compliance Monitoring Process.Levels of Non-Compliance.4. This should correct the numbering of vi and vii</p>	

Name	Company	Comments	Drafting Team Response
Scott McCoy	Xcel Energy	<p>Section 1303, under Measures (4) (iv) has minimum criteria for types of checks, but this is worthless without requiring some form of denial criteria. While (4) (v) does mention adverse actions, it is not intuitive that this is a criterion for denial of employment based on a set criterion. This should not be prescriptive either, but spelling out that the company should have a written denial criteria that is uniformly enforced should be added for both clarification and to ensure that the purpose of conducting background screenings is accomplished.</p> <p>Section 1303, Requirement (4) the phrase "prior to being granted unrestricted access to critical assets" should be removed since it conflicts with Section 1305, "When physical perimeters are defined, different security levels shall be assigned to these perimeters depending on the assets within these perimeter(s).</p> <p>Section 1303, Requirement (4) (vi) is unnecessary and an unreasonable administrative and costly requirement. For cause is justified, but renewing a background check every five years serves no point, especially when this standard does not require a company to take action based on derogatory information.</p> <p>Section 1303, Requirement (4) (iii) Access revocation within 24 hours is not a practical requirement. Even assuming that a company has these processes automated, it is an unrealistic target, especially considering that contract workers are included and it is more difficult to even interpret when they have technically left.</p>	

Name	Company	Comments	Drafting Team Response
Seiki Harada	BC Hydro	1303 Personnel & Training, Canadian law generally prohibits, and makes it an offence, to use or even communicate the Social Security Number (in Canada called Social Insurance Number) for any purposes other than as required or authorized by law in connection with the administration or enforcement of the Income Tax Act (Canada). Hence, the words "Social Security Number" should be replaced with "an appropriate identity".	References to SSN and SIN have been eliminated in favor of identity verification.

Name	Company	Comments	Drafting Team Response
Shelly Bell	San Diego Gas & Electric	<p>4. RE: NERC 1300 draft, section 1303 (4) (iv) and (vi)</p> <p>Comment: Requirements are discussed in this section regarding background screening. Since ongoing background screening of existing employees is prohibited by our state laws under most conditions, we have a concern about this sort of periodic background screening. The statement "as permitted by law and subject to existing collective bargaining unit agreements" may render this requirement impotent in certain regions, such as California. The language should be clarified to accentuate the importance of the requirement without making compliance impossible.</p>	<p>California law does not preclude up-date screening as long as appropriate FCRA paperwork is on file.</p>

Name	Company	Comments	Drafting Team Response
Stacy Bresler	PacifiCorp	1303.1.2 Does "training" require any form of certification, NERC or otherwise? Please elaborate training requirements.	<p data-bbox="1310 164 1650 188">Training certification is not required.</p> <p data-bbox="1310 220 1841 336">This section is left to company discretion, as long as the elements in 1303 are covered. It is intentionally non-prescriptive to allow companies flexibility in developing their in-house training.</p>

Name	Company	Comments	Drafting Team Response
Terry Doern	BPA	<p>1303.a.1 BPA Transmission is in agreement with the WECC EMS WG's comment: Replace "personnel subject to the standard " to "personnel having access to critical cyber assets".</p> <p>BPA comment - We are looking to ensure that persons who have been identified by the utility/agency as being of a certain risk level, should have the appropriate training.</p> <p>1303.I.4 Section (iv): Each utility/Agency should define the level of check required. In our case, those who are identified as being Level 2 security positions by OPM's (U.S Office of Personnel Management) definition, will require a level of background check and possibly federal clearance that will be defined by the agency.</p> <p>Also note that SSN or SIN checks are not good enough to detect problems, even when coupled with Criminal checks. We find that doing a credit history, job history and education check often provides information that would not have been revealed by the SSN and Criminal checks. There is also no mention of verification of citizenship or association with terrorist sponsoring countries here.</p> <p>The minimum SSN &amp; 7 yr criminal checks they prescribe may be in conflict with "federal, state, provincial, and local laws." Add a clause "where allowed by federal, state, provincial, and local laws."..</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: Access revocation is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>In Canada, the equivalent is the Social Insurance Number (SIN) and should be added.</p> <p>1303.n.2 Item 2. It may be legally problematic to keep certain documents. Some flexibility needs to be built into this section. Records may, for example, be maintained by a contracted background checking organization rather than the agency. This would relieve the agency of legal liability for the sensitive documents while still allowing them access when required.</p>	Please see responses to Jim Hiebert, WECC EMS WG.



Name	Company	Comments	Drafting Team Response
Tom Flowers	Centerpoint Energy	<p>Page 13, 1303 Personnel &amp; Training</p> <p>General comment:</p> <p>This section needs to clearly identify the types of access:</p> <p>Physical :</p> <ol style="list-style-type: none"> <li>1. Unescorted Access</li> <li>2. Escorted Access</li> <li>3. Unauthorized/Illegal</li> </ol> <p>Cyber:</p> <ol style="list-style-type: none"> <li>1. Authorized</li> <li>2. Unauthorized</li> </ol> <p>Specific Comments:</p> <p>Page 13, (a)(4) Requirements</p> <p>Delete "unrestricted" from the second sentence.</p>	<p>Access control encompasses both physical and cyber access to critical cyber assets, as defined by the standard.</p> <p>Unrestricted will be changed to authorized.</p>

Name	Company	Comments	Drafting Team Response
Tom Pruitt	Duke Energy	<p>1303 Administrators should have a higher level of security awareness on a particular system, but not necessarily a higher level of training or screening than an operator.</p> <p>1303 Background checks are not defined by the requirements, but are defined by the measure. The measure should not be more restrictive than the requirement.</p> <p>1303(4)(vi) Requiring re-screening every 5 years is unreasonable and would have a significant administrative cost not to mention an employee relations impact. It is reasonable to perform re-screening for cause.</p> <p>1303(a)(4) Does this apply to current employees as well as new employees?</p> <p>1303(b) This should be labeled as (b)</p> <p>1303(b)(1), pg 13 Suggest that this reinforcement be done on an annual basis to reduce administrative overhead of implementing this standard. It is not clear whether the reinforcement is to be the only training (I don't think that's what is intended but it is not clear how often the training should be conducted and quarterly reinforcement is too often). How is this to be measured?</p> <p>1303(b)(2) Suggest that the training be annually with reinforcement between training cycles.</p> <p>1303(b)(2)(ii) Does this mean operators (users), administrators, or both?</p> <p>1303(b)(4)(i) What type of access? User access? There are NUMEROUS users w/ USER access to systems in a power plant. Administrative rights? This is much more manageable.</p> <p>1303(b)(4)(ii) 2 business days is unreasonable for a large generation station, especially for USER access. 2 weeks would be a more manageable timeframe. This is assuming that "any substantive" means any 1 person?</p> <p>1303(b)(4)(iii) If a person is terminated, they are no longer allowed unescorted access to a generation station. Two business days is unreasonable for other changes, such as a transfer. Two weeks would be a more manageable timeframe. The "within 24 hours" should only</p>	<p>1303 Administrators' level of security awareness should be up to company discretion. Section 1303 sets minimums.</p> <p>1303 Background checks -- Requirements set the high-level tone and the measures provide the detail.</p> <p>1303(4)(vi) The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's.</p> <p>1303(a)(4) Please see FAQ 1303 #1</p> <p>1303(b) The standard will be reformatted</p> <p>1303(b)(1), pg 13 Security awareness can be accomplished through a variety of media and should not be onerous.</p> <p>Measurement can be accomplished by providing documentation that security awareness reinforcement has been conducted (e.g., e-mails, memos, posters, sign-in sheets, etc.)</p> <p>1303(b)(2) Changed to reflect annual training.</p> <p>1303(b)(2)(ii) and 1303(b)(4)(i) Any authorized person with access to a critical asset, as defined in the Standard.</p> <p>1303(b)(4)(ii) and 1303(b)(4)(iii) Changed to 24 hours for terminations for cause, and 7 calendar days for other personnel actions.</p> <p>1303(l) Standard will be reformatted</p>

Name	Company	Comments	Drafting Team Response
		<p>apply to terminations or required transfer. Other changes due to normal reassignments should be longer and the 10 business day period suggested by others is reasonable. For consistency, all changes to all types of access lists should be changed within 24 hours and normal work reassignments within 10 business days. Suggested re-wording: "Access revocation must be completed within 24 hours for any personnel who have a change in status where they are not allowed access to critical cyber assets, due to required transfers or terminations. Access revocation must be completed within 10 business days for any personnel who have a change in status where they are not allowed access to critical cyber assets due to normal transfer."</p> <p>1303(l) Should have been (b) - cross references between sections is messed up. Sections are labeled xxxx (a) (bb) but referenced xxxx.a.bb. Suggested change: (b) Measures</p>	

Name	Company	Comments	Drafting Team Response
William Smith	Allegheny Energy	<p>3. 1303 – Personnel &amp; Training</p> <p>Personnel having access to critical cyber assets should not be required to have a higher level of screening than other employees, as long as screening performed for all employees is at a sufficient level for those with access to critical cyber assets.</p> <p>If contractors and vendors are included in the standard, they should specifically be mentioned as part of "personnel".</p> <p>Also, generating stations operations do not generally allow for background screening for ALL personnel, especially contractors, accessing critical cyber access areas, such as control rooms. Since generating station personnel typically staff this area, background screening should not be required.</p>	<p>Up to company discretion. Section 1303 sets minimums.</p> <p>Contractors and vendors are referenced in 1303 (a)(4) and FAQ 1303 #1.</p> <p>The Standard is intended to create a higher level of trustworthiness for personnel having access to critical assets and to guard against potential insider threats. Periodic revalidation is an element of this level of vetting, similar to that found in nuclear and other sensitive positions. The timeline requirements are consistent with the FCRA and further guidance is found in the publication referenced in the FAQ's. If contractors and others who are not cleared require access to critical cyber assets, they would need to be escorted.</p>

# Section 1304 Comments and Drafting Team Responses

Name	Company	Comments	Drafting Team Responses
A. Ralph Rufrano	NYPA	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;  "The responsible entity shall ensure that all documentation reflect current configurations and processes."  to  The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from; "The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	<p>1304.a.2, An appropriate use banner is part of best practices for interactive access and is a requirement to enable follow-up on incident response. Without such a banner, any follow-up action on incident investigation may not be legal.</p> <p>1304 a.2 The standard requires that the entity ensure that all aspects in a control are implemented. Effective implementation of a control must include consideration of all three components. The language in the current proposed standard adequately expresses this requirement.</p> <p>1304 a.3 The standard requires that the entity ensure that all aspects in a control are implemented. Effective implementation of a control must include consideration of all three components. . The language in the current proposed standard adequately expresses this requirement.</p> <p>1304 a.4 The wording in the standard will be amended to clarify the applicability.</p> <p>Compliance Monitoring Process; 1304.d.3 NERC receives aggregate information from the Regional Organizations. Certification documents of the individual entity and any audit results are retained by the Regions. It is intended for the supporting documents to be inspected on site at the entity and remain in physical possession of the entity.</p> <p>This section of the standard will be modified to clarify this paragraph: Required documents exist, but records for some transactions are missing.</p>

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance

"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

Name	Company	Comments	Drafting Team Responses
Al Cooley	Verano	<p>1304, Page 17, a, 2, Electronic Access Controls: In order to ensure the perimeter is not breached, authentication should be carried out before the external communication comes in contact with electronic resources within the perimeter. Otherwise it is possible to penetrate the system before authentication takes place. To preclude this scenario, the following could be appended to the last sentence in the first paragraph "...to ensure authenticity of the accessing party, and such authentication shall be carried out before any communication received from the external party is allowed to interact with any asset within the logical perimeter."</p> <p>1304, Page 17, a, 2, Electronic Access Controls: Recognizing the fact that most organizations employ strong technology to manage logical access, many malicious intruders focus their penetration efforts on embedding payloads in legitimate traffic. As a result, technologies at the electronic perimeter are now designed to detect and automatically block such malicious payloads, in addition to managing logical access. The importance of this protection does not appear to come out at present. This section focuses on logical access control, and the section on "Integrity Software" is focused on possible system level tools. While system level integrity tools are both desirable and complementary, in many cases the need for CPU cycles, predictability and/or vendor support may preclude deployment of CPU intensive Integrity Software (e.g. AV, IPS) on the systems themselves. Presumably that is the reason why that section calls for a process governing deployment, rather than directly requiring deployment of the protection software? Consequentially, it would seem desirable to explicitly call out the need for monitoring authorized traffic for malicious payloads at the perimeter, and blocking such payloads. This could be accomplished by adding the following after the second sentence, "They will also ensure that authorized traffic does not contain malicious embedded content."</p> <p>1304, Page 21, f, Sanctions: Despite the efforts of many parties to address the issue of cyber security in the nation's critical infrastructure, our progress as an industry in making substantive changes has been modest. The standard must provide compliance incentives that are meaningful enough that the security issue receives appropriate attention. 1300 should have mandatory non-compliance penalties that are substantial enough to be meaningful within the context of a specific non-complying entity's financial performance, while not being onerous to other entities. As such penalties should be scaled.</p>	<p>1304 a, 2. This requirement refers to authentication at access points to the electronic perimeter. By definition, access to the perimeter must be obtained before accessing assets within the perimeter.</p> <p>1304, a, 2, This section of 1304 deals with access control. Detection of malicious or inappropriate payload or content is an intrusion detection and data integrity issue. The standard requires that the entity implement appropriate measures to monitor and detect intrusions.</p> <p>1304, f, Sanctions The comments have been noted will be considered at the appropriate time.</p>

Name	Company	Comments	Drafting Team Responses
Allen Berman	LIPA	1304 Electronic Security (a)Requirements (1)Electronic Access Controls Comment: Please clarify what is meant by the following statement. “Electronic access control devices shall display an appropriate use banner upon interactive access attempts.”	The FAQ document will include examples of banners extracted from other best practice documents.



Name	Company	Comments	Drafting Team Responses
Bill Wagner	Calpine	<p>Page 17, 1304 Electronic Security, (a) Requirements, (2) Electronic Access Controls, last sentence in first paragraph of this section "strong procedural or technical measures" provide definition or for meaning of "strong."</p> <p>Page 17, 1304 Electronic Security, (a) Requirements, (3) Monitoring Electronic Access Control: It may be useful to differentiate between Active Monitoring (real-time) as opposed to Passive Monitoring. This paragraph could be interpreted as 24x7 Passive Monitoring (where records of incidents are written to logs but are not reviewed in real time). It seems the intent is for active 24x7 monitoring where the event is proactively detected and responded to in near real time.</p>	<p>1304 Electronic Security, (a) Requirements, (2) In section 1304 of the FAQ document, the response to Question 5 explains what is meant by strong authentication with examples. This section and the FAQ will be amended to clarify the requirement.</p> <p>1304 Electronic Security, (a) Requirements, (3) The measures section requires the entity to implement measures to report and alert on unauthorized access or attempts at unauthorized access.</p>

Name	Company	Comments	Drafting Team Responses
Charles Yeung	SPP	<p>1304 (a) (4) Documentation Review and Maintenance: Define "timely." Term is too vague and subjective. Needs to be consistent with 1304 (b) (4) Documentation Review and Maintenance.</p> <p>1304 (b) (4) Documentation Review and Maintenance: 90 days to update the referenced documents is excessive, certainly not "timely." Maximum of 30 days is recommended.</p>	<p>1304 (a) (4) The corresponding measures section specifies what "timely" means.</p> <p>1304 (b) (4) It is the drafting team's consensus that 90 days is appropriate. This is consistent with measures in other sections of the standard.</p>

Name	Company	Comments	Drafting Team Responses
Charlie Salamone	NSTAR	1304.a.2 - Clarify that this screen is intended for the user to see, saying essentially that they should "follow policy". Insert language similar to "where technically feasible" to recognize that some older equipment cannot be made to display such screens.	1304.a.2 The standard will include a technical feasibility clause.

Name	Company	Comments	Drafting Team Responses
Chris DeGraffenried	NYPA	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance

"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

Name	Company	Comments	Drafting Team Responses
Dave McCoy	Great Plains Energy	<p>1304 - Question 5 in the Frequently Asked Questions defines strong authentication which is referenced in Standard 1304 as requiring at least two-factor identification. In a controlled office environment that already has physical access controls in place, it would seem that single-factor identification such as a password would be adequate. Question 5 also states that strong authentication be implemented for interactive access to an electronic security perimeter. This raises a couple of questions: 1) Is strong authentication only required for external interactive access? If so, please clarify external access. Is this referring to a remote access connection such as a VPN?</p> <p>2) Is strong authentication required for interactive access from a network segment outside the electronic security perimeter, but within a controlled office environment that has physical access controls in place?</p>	Any interactive access from any point outside the electronic perimeter requires strong authentication.

Name	Company	Comments	Drafting Team Responses
Dave Norton	Entergy Transmission	<p>27. Page 17: No specifications or qualifications are provided as to how non-critical assets operating within the defined electronic security perimeter must comply with the requirements of this standard. The implication is that they be treated as critical. Some differentiation is needed between treatments of non-critical versus critical assets with the same electronic security perimeter.</p> <p>28. Page 17 - 1304 third bullet: The standard requires "the implementation of processes, tools, and procedures to monitor electronic (logical) access to the perimeter(s) and the critical cyber assets." This could have serious adverse performance implications for EMS/SCADA host systems. Is it expected that every keystroke and click be logged? What, exactly, must be logged?</p> <p>29. Page 17 - 1304 (a) Requirements (2) second paragraph. What is an "appropriate use banner"?</p> <p>30. Page 19 - 1304 (e) Levels of Non-Compliance, Level One and Level Two and Level Three. The level one non-compliance for a gap in access records of &lt; 7 days is a more serious situation than the Level Two and the Level Three, ...and/or...Access not monitored to any critical asset for less than one day. Level Three: ...for more than one day but less than one week; or...</p>	<p>27. If non-critical cyber assets cannot be separated from critical cyber assets in separate electronic perimeters, those non-critical cyber assets are subject to the same perimeter access control requirements.</p> <p>28. The requirement is to monitor logical access, not keystrokes or mouse clicks. The standard requires logging of access control events.</p> <p>29. The FAQ document will include examples of banners extracted from other best practice documents.</p> <p>30. The levels of compliance for monitoring access records will be corrected.</p>

Name	Company	Comments	Drafting Team Responses
David Kiguel	Hydro One	<p>1304 a.2 Electronic Access Controls: The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s).</p> <p>-----</p> <p>1304 a.3 Monitoring Electronic Access Control: The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized</p> <p>-----</p> <p>Compliance Monitoring Process Change; 1304 d.3 The responsible entity shall make the following available for inspection by the compliance monitor upon request:</p> <p>to</p> <p>The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements and obligations: 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>-----</p> <p>1304 a.4 Change - The responsible entity shall ensure that all documentation reflect current configurations and processes.</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304 a 1 through 1304 a.3 reflect current configurations and processes.</p> <p>-----</p> <p>1304 a.4 Remove -The entity shall conduct periodic reviews of these</p>	Please see response to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Responses
		documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here) -----	
		Level of non compliance Level three Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified	

Name	Company	Comments	Drafting Team Responses
David Little	Nova Scotia Power	<p>1304</p> <p>1304 a.2 Electronic Access Controls: The responsible entity shall implement a combination of organizational, add and/or technical, add and/or procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s).</p> <p>1304 a.3 Monitoring Electronic Access Control: The responsible entity shall implement a combination of organizational, again add and/or technical, add and/or procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized</p> <p>Change 1304 a.4 from; The responsible entity shall ensure that all documentation reflect current configurations and processes. to The responsible entity shall ensure that all documentation required comply with 1304 a 1 through 1304 a.3 reflect current configurations and processes.</p> <p>1304 a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from; The responsible entity shall make the following available for inspection by the compliance monitor upon request: to The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:</p> <p>Level of non compliance Level three-Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified.</p>	Please see response to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	(a) Requirements - Although this may be addressed in other NERC guidance, there appears to be no identification of data types or attributes (numeric/alphanumeric, range checks, maximum deviation allowances, etc.) associated with information crossing perimeter boundaries. This, along with appropriate security MOAs/MOUs executed with communication partners would promote security by providing guidelines for the acceptance of data and criteria/procedures for addressing potential security incidents between partners. It should be considered that the “bad guy” does not have to perform direct attacks against the entity’s system, he may have broken into a partner’s system and be sending bad data, out-of-bounds commands, or contaminated files to the entity through a “trusted” channel.	Application level security is not addressed by this standard.

Name	Company	Comments	Drafting Team Responses
Dennis Kalma	AESO	1304 a .1. Requirements: The team needs to reconsider this part in view of the volume of work associated to this section.	The team will consider this comment in the implementation plan.

Name	Company	Comments	Drafting Team Responses
Ed Riley	CAISO	<p>1304.a.2 Strong is a subjective term and needs to be clearly defined.</p> <p>Add “where equipment supports banners” to the end of the last sentence to read “...use banner upon interactive access attempts, where equipment supports banners.”</p>	<p>In section 1304 of the FAQ document, the response to Question 5 explains what is meant by strong authentication with examples. The standard and FAQ document will be amended to clarify this requirement.</p> <p>The standard will include a technical feasibility clause.</p>

Name	Company	Comments	Drafting Team Responses
Ed Stein	First Energy	<p>1304 – Electronic Perimeter</p> <p>Page 17 (a) (1) Electronic Security perimeter: Proposed language states “Communication links ...are NOT part of the secured perimeter...However, end points of the communication links... are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements...” Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.</p> <p>Page 18: (b) (1) Electronic Security Perimeter: ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD’s) and modems connected to cyber assets. Are these considered “access points to the electronic security perimeter”?</p> <p>If the FRAD’s are considered ‘within the perimeter’ with the resulting requirements extending to the FRAD’s, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.</p> <p>Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.</p> <p>P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if “...not all transactions documented have records.” ABC seeks clarification. If a transaction is documented, by definition, doesn’t that mean the transaction has a record?</p> <p>Page 17 Electronic Access Controls: “...non critical cyber assets (within the perimeter) must comply with the requirements of this standard.” Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.</p>	<p>Page 17 (a) (1) The standard specifically excludes communication links.</p> <p>Page 18: (b) (1) Electronic Security Perimeter: Frame Relay Access Devices and modems connected to cyber assets are considered access points if they are part of the electronic perimeter, not inside the perimeter.</p> <p>Page 18: Measures (3): This section will be reformatted for clarity.</p> <p>P. 19 (e) (3) Required documents exist, but records for some transactions are missing. This section of the standard will be modified to clarify this paragraph.</p> <p>Page 17 Electronic Access Controls Non-critical cyber assets (within the perimeter) must comply with the requirements of this standard.</p>

Name	Company	Comments	Drafting Team Responses
Francis Flynn	National Grid	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>1304.a.2 Electronic Access Controls: change to: The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s).</p> <p>Change 1304.a.2 from: These controls shall implement an access control model that denies access by default unless explicit access permissions are specified.</p> <p>to:</p> <p>Where capable, these controls shall implement an access control model that denies access by default unless explicit access permissions are specified.</p> <p>Change 1304.a.2 from: ...the responsible entity shall implement strong procedural or technical measures to ensure authenticity of the accessing party.</p> <p>to:</p> <p>...the responsible entity shall implement procedural or technical measures to ensure authenticity of the accessing party.</p> <p>1304.a.3 Monitoring Electronic Access Control: change to: The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized</p> <p>Change 1304.a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p>	<p>Please see response to A. Ralph Rufrano.</p> <p>1304.a.2 Electronic Access Controls In perimeter defense, the default posture must be to deny access. Strong authentication is required for interactive access to the perimeter.</p> <p>1304.b.2 Devices of the same type may implement different access control policies and configurations. The entity may group devices with the same policy and configurations as appropriate in their documentation.</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Change 1304.b.2 from: ...procedural controls for logical (electronic) access and their implementation for each electronic access point</p> <p>to:</p> <p>...procedural controls for logical (electronic) access and their implementation for each type of electronic access point.</p> <p>Change 1304.b.2 from: For each control, the document or set of documents shall identify and describe, at a minimum...</p> <p>to:</p> <p>For each type of control, the document or set of documents shall identify and describe, at a minimum...</p> <p>Change 1304.b.3 from: ...technical controls and their supporting documents implemented to verify access records for authorized access against access control rights...</p> <p>to:</p> <p>...technical controls and their supporting documents implemented to verify access records for authorized access against access control rights for each control...</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p> <p>to</p>	



Name	Company	Comments	Drafting Team Responses
		<p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"</p>	
		<p>1304.e.3 Level of non compliance            "Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.</p>	
		<p>Change 1304.e.3 from: Document(s) exist, but one or more access points have not been identified or the document(s) do not identify or describe access controls for one or more access points or</p>	
		<p>to:</p>	
		<p>Document(s) exist, but one or more access points have not been identified or the document(s) do not identify or describe access controls for one or more types of access points or</p>	

Name	Company	Comments	Drafting Team Responses
Francois Lemay	Brascan Power	Make section 1304.1 more consistent with its physical security counterpart 1305.a by: (A) adding section 1304.a.6 "Maintenance and testing of electronic security systems", and (B) adding (or moving from standard 1306) section 1304.a.5 "Logging electronic access"	1304 deals with the electronic security perimeter. Testing has been more logically put in 1306 with general testing and assurance requirements. Logging specifically as a means of monitoring access has been treated here. General logging requirements are described in 1306.

Name	Company	Comments	Drafting Team Responses
Gary Campbell		<p>1304</p> <p>Measures</p> <p>A document is not required in the sections under requiements but here we are measuring for it.</p> <p>1 - How can document verify that all critical assests are within the electronic security perimeter? Suggest rethinking.</p> <p>4 Are the number references used correct? I can not follow them easily.</p> <p>Levels of Compliance</p> <p>Please define documents. Which or what documents am I looking for.</p> <p>Level 4</p> <p>Please be more explanantory.</p>	<p>Measures</p> <p>Documents are used to measure the entity's compliance to the requirements. This sentence will be reworded to clarify the intent.</p> <p>The draft standard's number references will be reviewed to ensure accuracy and correctness after formatting</p> <p>Levels of Compliance</p> <p>Documents can be hard copy or electronic and can include policy manuals, procedures, diagrams and/or architectural descriptions.</p> <p>Documents required by the standard cannot be produced for review, nor evidence (such as logs) of monitoring of access.</p>

Name	Company	Comments	Drafting Team Responses
Guy Zito	NPCC	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"</p> <p>Level of non compliance</p> <p>"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.</p>	

Name	Company	Comments	Drafting Team Responses
Jim Hiebert	WECC EMS WG	<p>1304.a.2 Strong is a subjective term and needs to be clearly defined.</p> <p>Add “where equipment supports banners” to the end of the last sentence to read “...use banner upon interactive access attempts, where equipment supports banners.”</p>	<p>1304.a.2 In section 1304 of the FAQ document, the response to Question 5 explains what is meant by strong authentication with examples. This section of the standard will be amended to clarify the requirement.</p> <p>The standard will include a technical feasibility clause.</p>

Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>1304 – Electronic Perimeter</p> <p>Page 17 (a) (1) Electronic Security perimeter: Proposed language states “Communication links ...are NOT part of the secured perimeter...However, end points of the communication links... are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements...” Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.</p> <p>Page 18: (b) (1) Electronic Security Perimeter: ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD’s) and modems connected to cyber assets. Are these considered “access points to the electronic security perimeter”?</p> <p>If the FRAD’s are considered ‘within the perimeter’ with the resulting requirements extending to the FRAD’s, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.</p> <p>Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.</p> <p>P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if “...not all transactions documented have records.” ABC seeks clarification. If a transaction is documented, by definition, doesn’t that mean the transaction has a record?</p> <p>Page 17 Electronic Access Controls: “...non critical cyber assets (within the perimeter) must comply with the requirements of this standard.” Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.</p>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
John Blazeovitch	Exelon	<p>1304.b.1</p> <p>The last sentence requires that the Electronic Security Perimeter document shall verify that all critical cyber assets are within the electronic security perimeter. The definition of a critical cyber asset includes software and data. If depicting software and data on a schematic is beyond the intent of the requirement, we recommend that the last sentence read: The document or set of documents shall verify that all critical cyber asset hardware is within the electronic security perimeter(s)</p>	<p>The standard requires that the document verify that systems hosting the critical software and data be within the electronic perimeter.</p>



Name	Company	Comments	Drafting Team Responses
John Hobbick	Consumers Energy	<p>1304 Electronic Security 3) Monitoring Electronic Access Control An exception should be allowed for those locations that have only dial up access.</p> <p>The measure for this section is confusing particularly the last sentence.</p> <p>Section 1304, first paragraph, discusses the assignment of different security levels for the electronic perimeter(s), yet fails to note how these different levels might result in different security requirements. This seems to imply different requirements based on levels might be applied (and should be) yet there is no further discussion.</p> <p>Section 1304, Subsection (a), Para (3), requires that access, authorized or unauthorized be monitored and detected. This is an unreasonable requirement for many substation equipment installations. Many dial-up-accessable pieces of equipment, such as relays, controllers, etc, that have a limited ability to effect overall system reliability, still might fall into the classification of Critical Cyber Assets. For these pieces of equipment, there is no reasonable solution to providing monitoring or detection. Efforts to attempt to satisfy this requirement, which might require a more network-type of connection, could even increase the susceptibility to unauthorized access. This requirement should either be deleted, or apply only to significant EMS-type or routable-protocol-types of installations.</p>	<p>1304 Electronic Security 3) Monitoring Electronic Access Control Dial-up access must be monitored for critical cyber assets.</p> <p>The sentence will be reformatted to clarify the measure.</p> <p>Section 1304, first paragraph The introductory paragraph is a general overview and this part is intended to explain that some assets are more critical than others, as is the case for those relating to the reliable operation of the bulk electric system.</p> <p>Section 1304, Subsection (a), Para (3) The answer to Question 3, Page 9, in the Section 1304 part of the FAQ document provides explanations that address this comment.</p>

Name	Company	Comments	Drafting Team Responses
Kathleen Goodman	ISO-NE	<p>1304 Preamble no requirement to view logs or "be alerted" as mentioned in the FAQ (page 10, question 6 "monitor access....and to be alerted so you can respond). Does monitor mean just mean logged, or viewed and acted upon, as necessary? Need better clarification of term "monitoring."</p> <p>1304 Compliance Monitoring Please state clearly that this is to be done with respect to applicable confidentiality agreements in place. This information can be highly sensitive.</p>	<p>NERC receives aggregate information from the Regional Organizations. Individual entity audit results are retained by the Regions. It is intended for the documents to be inspected on site at the entity and remain in physical possession of the entity.</p>

Name	Company	Comments	Drafting Team Responses
Ken Goldsmith	Alliant Energy	<p>1304 Electronic Security</p> <p>Article a-1 Stating non-critical cyber assets within the defined electronic security perimeter must comply with the requirements of this standard is excessive. There should be security controls in place to mitigate any impact to a critical cyber asset, but it should not be required to comply with this standard.</p> <p>Article a-2 Electronic access control devices shall display an appropriate use banner upon interactive access attempts. . . . is good security but it does not seem appropriate for a NERC standard and it is not always technically feasibly. Request it be removed.</p>	<p>Article a-1 If non-critical cyber assets cannot be separated from critical cyber assets in separate electronic perimeters, those non-critical cyber assets are subject to the same access control requirements.</p> <p>Article a-2 An appropriate use banner is part of best practices for interactive access and is a requirement to enable follow-up on incident response. Without such a banner, any follow-up action on incident investigation may not be legal.</p> <p>The standard will include a technical feasibility clause.</p>

Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	<p>Section 1304</p> <p>(a)(2)(2nd parag.)</p> <p>Clarify that the specified screen is intended for the user to see, saying essentially that they should “follow policy”.</p> <p>The sentence should begin: “Where technically feasible, electronic access.” This will recognize that some older equipment cannot be made to display such screens</p> <p>(e)(2)(2nd parag.) – The phrase “for less than one day” is unclear in context – substitute “Access to any critical cyber asset remains unmonitored for some period that does not exceed 24 hours.”</p>	<p>(a)(2)(2nd parag.) The term “interactive logical access” addresses this comment. The banner is also intended to be seen by users who may not be aware of policy: the banner attempts to summarize this policy for these users</p> <p>(e)(2)(2nd parag.) The phrase will be amended in the standard with corrections in this section of the 1304.</p>

Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>1304 – Electronic Perimeter</p> <p>Page 17 (a) (1) Electronic Security perimeter: Proposed language states “Communication links ...are NOT part of the secured perimeter...However, end points of the communication links... are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements...” Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. Cinergy seeks clarification.</p> <p>Page 18: (b) (1) Electronic Security Perimeter: Cinergy seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD’s) and modems connected to cyber assets. Are these considered “access points to the electronic security perimeter”?</p> <p>If the FRAD’s are considered ‘within the perimeter’ with the resulting requirements extending to the FRAD’s, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.</p> <p>Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.</p> <p>P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if “...not all transactions documented have records.” Cinergy seeks clarification. If a transaction is documented, by definition, doesn’t that mean the transaction has a record?</p> <p>Page 17 Electronic Access Controls: “...non critical cyber assets (within the perimeter) must comply with the requirements of this standard.” Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.</p>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Linda Campbell	FRCC	<p>1304 Electronic Security</p> <p>The opening paragraph of this section introduces a concept of assigning security levels to electronic perimeters; however, this does not follow through the remainder of the document. We recommend this be stricken as it does not add value to the standard.</p> <p>(a) (1) Electronic security perimeter It is unclear from the wording in this section what is meant by the terms “access point” and “end point”. The following wording might make this section more clear (the term “access point” is also a candidate for the definitions section):</p> <p>.....The responsible entity shall identify the electronic security perimeter(s) surrounding its critical cyber assets and all access points (firewalls, routers, modems, etc) into the perimeter(s). Omit the sentence, “Communication links connecting discrete electronic perimeters are not considered part of the security perimeter.” Omit sentence, “Where there are also non-critical cyber assets..... “ These previous sentences do not have anything to do with the perimeter.</p> <p>(a) (2) Electronic access control The FAQ refers to dial-in modems that have “proper access control and logging”. The requirements need to be better defined. We know of no dial back modems that are designed for the substation environment (e.g. must be DC powered and capable of handling severe electrical surge). We have tried to use office style modems (Hayes, US Robotics, etc.) in substation will no success. The more rugged modems do not have any security features. We rely on password protection in the data switch, but they have no logging capability. How would this be addressed?</p> <p>Also, if we are allowing access into the electronic security perimeter through a router, what do we need to do at the router to implement “strong procedural or technical measures to ensure authenticity”? A router or firewall will typically filter access based upon IP address, and a firewall can enforce session authentication (login) before access to the perimeter is allowed. The FAQ for this section (question 5) seems to imply that two factor authentication is required, which is not practical in many situations, and certainly not possible with many of the devices, such as modems which are in the field today.</p> <p>What is an “interactive access attempt” and how does it differ from an “access attempt”?</p>	<p>The introduction provides an overview and clarifies the requirement to have a defined electronic security perimeter for critical cyber assets.</p> <p>(a) (1) Electronic security perimeter The term access point as it refers to a perimeter is self explanatory.</p> <p>The sentences suggested for omission are intended to clarify the scope of the section.</p> <p>(a) (2) Electronic access control The section on strong authentication will be further clarified in the standard.</p> <p>An “interactive access attempt” is an access attempt which allows interactive request and responses. This usually implies that there is an entity reading and responding to the access control device. Examples of appropriate use will be provided in the FAQ. The standard will also include a technical feasibility clause.</p> <p>(a)(4) The corresponding measures section specifies what “timely” means.</p> <p>(b) (4) References will be corrected.</p>

Name	Company	Comments	Drafting Team Responses
		<p>“appropriate use banner” – please define.. If what I think it is, not all systems are technically capable of presenting such a banner.</p>	
		<p>(a)(4) States that changes to documents shall be updated “in a timely fashion” should be changed to some periodicity. The Compliance section 1304(d)(3)(iv) gives a timetable of within 90 days of a modification.</p>	
		<p>(b) (4) references to 1304.2... refer to sections that don’t exist.. check the numbering.</p>	
		<p>(d) (2) Eliminate exceptions in the sentence, “keep document revisions and exceptions and other security” – requirements don’t mention exceptions. Change “other audit records such as access records” to “other access logs”</p>	
		<p>(e) The levels of noncompliance seem to be inconsistent. Level one is gap in logs for less than 7 days, but level 2 is no monitoring for 1 device for less than 1 day. It would appear that missing logs for 7 days is worse than not monitoring for less than 1 day, yet is a lower level of non-compliance.</p>	

Name	Company	Comments	Drafting Team Responses
Lyman Schaeffer	Pacific Gas & Electric	<p data-bbox="598 172 842 196">1304 Electronic Security:</p> <p data-bbox="598 228 1283 418">Again, we appreciate the standard giving each company the flexibility to conduct its own risk assessment and take action based on that process. However, this section appears to establish a standard on what measures are required at a given facility regardless of what that risk assessment determines. This appears to be a one size fits all approach which requires the entity to impose expensive monitoring requirements on assets where there are few, if any, risks.</p>	<p data-bbox="1314 172 1864 253">The standard, including this section, clearly applies to critical cyber assets as determined by the risk assessment process.</p>



Name	Company	Comments	Drafting Team Responses
Michael Allgeier	LCRA	1304 Electronic Security Given a local only sub-station network, if connected to a device like an SEL 2030 which is then connected to another SEL 2030 in another sub-station local only network, considered a routable network in this Standard? The networks are separated by devices which do not 'route' packets but you could login and then possibly telnet to the internal LAN. Example: Substation LAN – SEL 2030 – WAN – SEL 2030 – substation LAN	If any one of the devices is a critical cyber asset, the electronic perimeter includes both devices and access points to the perimeter fall within this standard. The devices may not use the routable protocol for operation or control, but if they are accessible using a routable protocol, (Telnet uses TCP/IP in this example), they qualify for inclusion in the standard.

Name	Company	Comments	Drafting Team Responses
Neil Phinney	Georgia Transmission Co	1304.a.2 Appropriate use banners can be invitations to hackers that there is something worthwhile behind the gate. There are situations where it is preferable to have blind access points. These should not be prohibited.	Banners may minimize displayed information which could be useful to potential intruders while satisfying requirements for forensic follow-up. Examples are provided in the FAQ.

Name	Company	Comments	Drafting Team Responses
Paul McClay	Tampa Electric Company	<p>1304 Electronic Security</p> <p>The opening paragraph of this section introduces a concept of assigning security levels to electronic perimeters; however, this does not follow through the remainder of the document. We recommend this be stricken as it does not add value to the standard.</p> <p>(a) (1) Electronic security perimeter It is unclear from the wording in this section what is meant by the terms “access point” and “end point”. The following wording might make this section more clear (the term “access point” is also a candidate for the definitions section):</p> <p>...The responsible entity shall identify the electronic security perimeter(s) surrounding its critical cyber assets and all access points (firewalls, routers, modems, etc) into the perimeter(s). Omit the sentence, “Communication links connecting discrete electronic perimeters are not considered part of the security perimeter.” Omit sentence, “Where there are also non-critical cyber assets..... “ These previous sentences do not have anything to do with the perimeter.</p> <p>(a) (2) Electronic access control The FAQ (for 1304) Q3 refers to dial-in modems that have "proper access control and logging". The fragment (paragraph 2) needs to be finished, not sure what this is supposed to be saying. However, the requirements for dial-in modems need to be better defined. We know of no dial back modems that are designed for the substation environment (e.g. must be DC powered and capable of handling severe electrical surge). We have tried to use office style modems (Hayes, US Robotics, etc.) in substation with no success. The more rugged modems do not have any security features. We rely on password protection in the data switch, but they have no logging capability. How would this be addressed?</p> <p>Also, if we are allowing access into the electronic security perimeter through a router, what do we need to do at the router to implement “strong procedural or technical measures to ensure authenticity”? A router or firewall will typically filter access based upon IP address, and a firewall can enforce session authentication (login) before access to the perimeter is allowed. The FAQ for this section (question 5) seems to imply that two factor authentication is required, which is not practical in many situations, and certainly not possible with many of the devices, such as modems which are in the field today.</p> <p>What is an “interactive access attempt” and how does it differ from an</p>	<p>The introduction provides an overview and clarifies the requirement to have a defined electronic security perimeter for critical cyber assets.</p> <p>(a) (1) Electronic security perimeter The term access point as it refers to a perimeter is self explanatory.</p> <p>The sentences suggested for omission are intended to clarify the scope of the section.</p> <p>(a) (2) Electronic access control The section on strong authentication will be further clarified in the standard.</p> <p>An “interactive access attempt” is an access attempt which allows interactive request and responses. This usually implies that there is an entity reading and responding to the access control device. Examples of appropriate use will be provided in the FAQ. The standard will also include a technical feasibility clause.</p> <p>(b) (4) References will be corrected.</p> <p>(d) (2) Exception data refers to data that is related to security exceptions. The sentence will be modified to refer to security incident related data. The more general term “audit record” is used here to include logs other than access logs (such as intrusion detection logs).</p> <p>(e) The standard will be re-drafted.</p>

Name	Company	Comments	Drafting Team Responses
		<p>“access attempt”?</p> <p>“appropriate use banner” – please define.. If what I think it is, not all systems are technically capable of presenting such a banner.</p> <p>(b) (4) references to 1304.2... refer to sections that don’t exist.. check the numbering.</p> <p>(d) (2) Eliminate exceptions in the sentence, “keep document revisions and exceptions and other security” – requirements don’t mention exceptions. Change “other audit records such as access records” to “other access logs”</p> <p>(e) The levels of noncompliance seem to be inconsistent. Level one is gap in logs for less than 7 days, but level 2 is no monitoring for 1 device for less than 1 day. It would appear that missing logs for 7 days is worse than not monitoring for less than 1 day, yet is a lower level of non-compliance.</p>	

Name	Company	Comments	Drafting Team Responses
Pedro Modia	FPL	<p>[Item 1 is very wordy and should be re-drafted to clearly articulate what the standard requires]</p> <p>The responsible entity shall ensure that all documentation reflect current configurations and processes. The entity shall conduct periodic reviews, as dictated by regular business process, of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes.</p> <p>The measure corresponding to this requirement specifies the frequency of the review.</p> <p>The responsible entity shall maintain a documentation or set of documents identifying...</p> <p>(3) Monitoring Electronic Access Control: The responsible entity shall maintain a document identifying organizational, technical, and procedural controls, including tools and procedures, for monitoring electronic (logical) access. This document shall identify supporting documents, including access records and logs, to verify that the tools and procedures are functioning and being used as designed. Additionally, the documentation or set of documents shall identify and describe processes...</p> <p>(d) Compliance Monitoring Process</p> <p>[Further clarification is required in regards to “investigations upon complaint.” How intrusive are these investigations, and what would predicate such investigations?]</p> <p>(1) The responsible entity shall demonstrate compliance through self-certification submitted to the compliance monitor annually. The compliance monitor may also use scheduled on-site reviews every three years, and investigations upon complaint, to assess performance.</p> <p>(ii) Records of electronic access to critical cyber assets (e.g., access logs, intrusion detection logs). [Please specify how long of a retention period is required for these.]</p> <p>Paragraph 2 of the compliance section specifies a retention period of at least 90 days.</p>	<p>The drafting team feels that the current wording adequately specifies the requirement.</p> <p>(3) Monitoring Electronic Access Control: The requirement specifies that the documents must not only identify the controls themselves, but must identify the documents which are produced to verify actual implementation of the controls. The current wording specifies this requirement.</p> <p>Compliance Monitoring Process (1) Investigations are part of NERC's Compliance Program. This is a standard NERC compliance monitoring process. The nature of the investigations depends on the complaint.</p> <p>(ii) Paragraph 2 of the compliance section specifies a retention period of at least 90 days.</p>

Name	Company	Comments	Drafting Team Responses
Pete Henderson	IMO	<p>1304 Electronic Security (a) Requirements (4) Documentation Review and Maintenance This should be reworded to, “The responsible entity shall ensure that all documentation required to comply with 1304 (a) (1) through 1304 (a) (3) reflects current configurations</p> <p>Delete the last sentence of this sub-section as it is redundant given 1304 (b) (4)</p>	<p>1304 Electronic Security (a) Requirements (4) Documentation Review and Maintenance</p> <p>Each section in the standard has stated documentation requirements for that section. It is implied that the requirement in each section applies to all documentation requirements for that section.</p> <p>1304 (b) (4) The last sentence specifies the requirement. 1304(b)(4) specifies the actual measures used for this requirement.</p>

Name	Company	Comments	Drafting Team Responses
Phil Sobol	SPP CIPWG	1304, (a), (2) The last sentence requires the use of a banner. Some existing systems may not be able to support a banner. Some qualifier should be added such as, where technically supported.	The standard will include a technical feasibility clause.

Name	Company	Comments	Drafting Team Responses
Ray A'Brial	CHGE	<p>From 1304.a.2, remove Electronic access control devices shall display an appropriate use banner upon interactive access attempts. because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to The responsible entity shall implement a combination of organizational, and/or echnical, and/or procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s).</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to The responsible entity shall implement a combination of organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>The responsible entity shall ensure that all documentation reflect current configurations and processes.</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>The responsible entity shall make the following available for inspection by the compliance monitor upon request:</p>	<p>Please see responses to A. Ralph Rufrano.</p> <p>(e)(2)(2nd parag.) The phrase for less than one day will be amended in the standard with corrections in this section of the 1304.</p>



Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:</p> <p>Level of non compliance  Level three-Supporting documents exist, but not all transactions documented have records - this part is ambiguous and should be clarified.</p> <p>(e)(2)(2nd parag.) – The phrase for less than one day is unclear in context – substitute Access to any critical cyber asset remains unmonitored for some period that does not exceed 24 hours.</p>	

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>1304 – Electronic Perimeter</p> <p>Page 17 (a) (1) Electronic Security perimeter: Proposed language states “Communication links ...are NOT part of the secured perimeter...However, end points of the communication links... are considered access points to the perimeter. Where there are non critical assets within the defined perimeter these non-critical assets must comply with the requirements...” Language is contradictory and confusing. Proposed language makes the asset and the end point critical assets and within the perimeter, but language excludes the communication line between them. The next sentence implies the communication line needs to be treated as though it is part of the perimeter. ABC seeks clarification.</p> <p>Page 18: (b) (1) Electronic Security Perimeter: ABC seeks clarification regarding from NERC regarding Frame Relay Access Devices (FRAD’s) and modems connected to cyber assets. Are these considered “access points to the electronic security perimeter”?</p> <p>If the FRAD’s are considered ‘within the perimeter’ with the resulting requirements extending to the FRAD’s, this is an excessive and unnecessary level of detail and will prove costly and burdensome without proven corresponding benefit.</p> <p>Page 18: Measures (3): Monitoring Electronic Access Controls: Wording of this section, particularly the last sentence, is very confusing and needs clarification regarding exact requirements for documentation and for implementation of monitoring the access controls.</p> <p>P. 19 (e) (3) Electronic Access Controls: Page 19 identifies a non-compliance item if “...not all transactions documented have records.” ABC seeks clarification. If a transaction is documented, by definition, doesn’t that mean the transaction has a record?</p> <p>Page 17 Electronic Access Controls: “...non critical cyber assets (within the perimeter) must comply with the requirements of this standard.” Different departments within the organization will handle different functions. Current language implies one rigid process to apply to both critical assets and non-critical assets, which may exist within the perimeter. Recommend that this be changed to: non-critical cyber assets within the perimeter must utilize similar electronic access controls.</p>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Richard Engelbrecht	Rochester Gas & Electric	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"</p> <p>Level of non compliance</p> <p>"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.</p>	

Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p>If standard protective relay systems are included, because of remote communication access, more detailed requirements need to be provided for the physical and electronic security perimeters of the dial-up access point. It appears the thrust of the standard is to address access to those cyber assets which could affect multiple facilities or components from a single access point. Using the example provided in the FAQ section 1304, question 3, access to a single RTU controlling a critical bulk asset in a substation, which doesn't use a routable protocol, does not require an electronic security perimeter at the RTU. It continues to say if a dial-up modem is used, an electric security perimeter is required just around the dial-up access point. Is the access point the location in the substation, or the remote terminal calling into the substation? It appears obvious that the access point mentioned above should be located inside the electronic security perimeter in the substation, but the standard does not specifically outline this concept. A similar analogy needs to be drawn for protective relay access. If protective relays in a substation do not use a routable protocol, do they only require a security perimeter around the dial-up access point in the substation? When addressing dial-up access, the discussion of security perimeters should be specific as to what requirements are for the local and remote access point.</p>	

Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p>General: If standard protective relay systems are included, because of remote communication access, more detailed requirements need to be provided for the physical and electronic security perimeters of the dial-up access point. It appears the thrust of the standard is to address access to those cyber assets which could affect multiple facilities or components from a single access point. Using the example provided in the FAQ section 1304, question 3, access to a single RTU controlling a critical bulk asset in a substation, which doesn't use a routable protocol, does not require an electronic security perimeter at the RTU. It continues to say if a dial-up modem is used, an electric security perimeter is required just around the dial-up access point. Is the access point the location in the substation, or the remote terminal calling into the substation? It appears obvious that the access point mentioned above should be located inside the electronic security perimeter in the substation, but the standard does not specifically outline this concept. A similar analogy needs to be drawn for protective relay access. If protective relays in a substation do not use a routable protocol, do they only require a security perimeter around the dial-up access point in the substation? When addressing dial-up access, the discussion of security perimeters should be specific as to what requirements are for the local and remote access point.</p> <p>Definition (Section 1304.a.2): What is meant by External interactive logical access?</p> <p>Section 1304.a.2.2nd paragraph: Clarify that this display is intended for the user to see, saying essentially that they should Follow Policy. Insert language similar to Where technically feasible in order to recognize that some equipment cannot be made to display such screens (e.g. substation electronic equipment).</p> <p>Section 1304.a.3: This section discusses the controls for monitoring authorized access and detecting unauthorized access. How does this apply for dial-up access? In the FAQ section 1304, question 3, the use of SCADA controlled, or dial-back modems, was listed as a means of electronic security perimeter. Dial-back modems would not necessary meet the requirements of Section 1304.a.3, as they do not usually provide logging capabilities. Additionally, dial-back modems have proven to be an insecure means of user authentication. From Schweitzer Engineering Laboratories paper, Attack and defend tools for remotely accessible control and protection equipment in electric power systems, available at <a href="http://www.selinc.com/techpprs/6132.pdf">http://www.selinc.com/techpprs/6132.pdf</a>, pg. 16. Dial-back security was once common in the electric power industry, but is no longer adequate because of dial-back spoofing.</p>	<p>General: The access point is at the receiving end of the dial-up access, which must e protected for a critical cyber asset.</p> <p>Definition (Section 1304.a.2) External interactive logical access" implies that access is requested interactively (by a person) by an entity outside of the perimeter. In these cases, strong procedural and/or technical measures are required to ensure authenticity.</p> <p>Section 1304.a.2.2nd paragraph: The standard will include a technical feasibility clause.</p> <p>Section 1304.a.3: The entity must ensure that equipment used will meet the requirements of the standard.</p>

Name	Company	Comments	Drafting Team Responses
		<p>Hackers have learned to fake the hang-up tone and remain on the line while the called modem attempts to dial its predefined dial-back number. Hackers just ignore the incoming dial tones and issue an answer tone that reestablishes connection to the dial-back modem. Thus, the dial-back has been spoofed or fooled into an unauthorized connection.</p>	

Name	Company	Comments	Drafting Team Responses
Robert Pelligrini	United Illuminating	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance

"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

Name	Company	Comments	Drafting Team Responses
Robert Snow		<p>In Electronic Security: Add denial of service protection as well as how to protect against transmissions not originating from the authorized control centers. The first would stop a control center from taking actions and the second would protect against others from operating the systems independent from the authorized control center.</p> <p>There should be some level of redundancy required to assure the systems function as required independent of cyber activity.</p> <p>The requirement for an Intrusion Assessment by an independent agency once every three years with the requirement that any vulnerabilities be remedied within three months.</p> <p>Adopt a "defence in depth" approach rather than what reads like one barrier around the system and nothing after an entity gets past the first barrier.</p>	<p>This standard addresses requirements in both access control and intrusion detection. Denial of service detection is typically part of an intrusion detection process.</p> <p>This standard does not address availability.</p> <p>1306, Systems Security Management, addresses requirements for regular vulnerability assessments.</p> <p>The standard as a whole addresses a complete security program which includes policies, procedures, perimeter defense and system and host level defense.</p>

Name	Company	Comments	Drafting Team Responses
Robert Strauss	NYSEG	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
------	---------	----------	-------------------------

to

"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"

Level of non compliance

"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>1304 (Electronic Security)</p> <ul style="list-style-type: none"> <li>• In (a)(1), the standard states that non-critical assets that are within the electronic perimeter must also comply with the requirements of the standard. What if all cyber assets within the perimeter can not comply (devices that do not log for instance)?</li> <li>• In (a)(2), the standard is not clear as to whether or not it is requiring strong, two factor authentication for interactive logical access. The FAQ (1304 Question 5) states it is a requirement, but the standard itself does not. In (1306)(a)(2)(i), the standard speaks to ‘in the absence of multi-factor access controls’. So it is unclear as to whether two factor authentication is or is not required.</li> <li>• Also in (a)(2), it states that all control devices SHALL display an appropriate use banner. Again, this can be implemented on most Unix/Windows hosts, but will every critical cyber asset be able to do this?</li> <li>• In (e)(1) and numerous other places throughout the standard, the measures are open-ended with no reasonable lower bound. In this case, any gap in access logs for less than 7 days is non-compliant. Does that include a 2 minute outage if you have to reboot your cardkey system? What about instances (such as storms/hurricanes/etc) where evacuations are ordered or your network is laying on the ground? Some grace period must be allowed.</li> <li>• (e)(2) is an open-ended measure with no reasonable lower bound. Again, some grace period must be allowed.</li> <li>• In (e)(3), not having a single access point documented out of potentially hundreds is a Level 3 non-compliance?</li> </ul>	<p>1304 (Electronic Security)</p> <p>(a)(1) Access control requirements in this section describe requirements for access control to the electronic perimeter. System logging requirements are addressed in Section 1306: exceptions because of legacy equipment not technically capable of providing logging must be documented.</p> <p>(a)(2) Two-factor authentication is one form of strong authentication. The standard only requires that you have strong technical or procedural measures, and the FAQ describes alternatives to technical implementations of two-factor authentication.</p> <p>The standard will include a technical feasibility clause for this section.</p> <p>(e)(1) The language used in the standard for this section will be clarified.</p> <p>(e)(2) The language used in the standard for this section will be clarified.</p> <p>(e)(3) Access points in a perimeter are gateways into the critical cyber assets within an electronic perimeter. A single compromise, failure or unmanaged access point compromises the perimeter.</p>

Name	Company	Comments	Drafting Team Responses
S. Kennedy Fell	NYISO	<p>From 1304.a.2, remove "Electronic access control devices shall display an appropriate use banner upon interactive access attempts." because it does improve security. This banner assists in legal matters.</p> <p>Change 1304 a.2 Electronic Access Controls: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls to manage logical access at all electronic access points to the electronic security perimeter(s) and the critical cyber assets within the electronic security perimeter(s)."</p> <p>Change 1304 a.3 Monitoring Electronic Access Control: to "The responsible entity shall implement a combination of organizational, "and/or" technical, "and/or" procedural controls, including tools and procedures, for monitoring authorized access, detecting unauthorized access (intrusions), and attempts at unauthorized.."</p> <p>Change 1304 a.4 from;</p> <p>"The responsible entity shall ensure that all documentation reflect current configurations and processes."</p> <p>to</p> <p>The responsible entity shall ensure that all documentation required comply with 1304.a.1 through 1304.a.3 reflect current configurations and processes.</p> <p>1304.a.4 Remove -The entity shall conduct periodic reviews of these documents to ensure accuracy and shall update all documents in a timely fashion following the implementation of changes. (This is a measure and should be removed here)</p> <p>Compliance Monitoring Process; Change 1304.d.3 from;</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request:"</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall make the following available for inspection by the compliance monitor upon request, subject to applicable confidentiality agreements:"</p> <p>Level of non compliance</p> <p>"Level three-Supporting documents exist, but not all transactions documented have records" - this part is ambiguous and should be clarified.</p>	

Name	Company	Comments	Drafting Team Responses
Stacy Bresler	Pacifcorp	1304.a.2 "...implement strong procedural or technical measures to ensure the authenticity..." appears to imply strong authentication is required. Strong authentication is also stated and clarified in the Cyber Security Standard (1300) Frequently Asked Questions (page 9, question 5) with respect to this 1304 standard. Please elaborate within the 1304 language exactly what is acceptable and unacceptable as forms of strong authentication.	Two-factor authentication is one form of strong authentication. The standard only requires that you have strong technical or procedural measures, and the FAQ describes alternatives to technical implementations of two-factor authentication. This section of the standard will be amended to clarify this requirement.



Name	Company	Comments	Drafting Team Responses
Terry Doern	BPA	<p>Reword “critical cyber assets reside and all access points to these perimeter(s)” to “critical cyber assets and all access points to the perimeter(s) reside.”</p> <p>Change “implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical assets within them” to “implementation of access control to critical assets within the logical security perimeter.”</p> <p>1304.a The phrase “access is controlled” should read “access should be controlled” (See the comments for Electronic Security Perimeter.</p> <p>The description of communication links and end points is ambiguous and seems to assume only hard wired infrastructure. Do microwave towers and communications equipment, and fall under this definition if they are the end points?</p> <p>1304.a.2 The statement “implement the organizational, technical, and procedural controls to manage logical access” is very nebulous. There are three types of controls: Management (sometimes known as Administrative), Operational (sometimes known as Physical), and Technical.</p> <p>Procedural controls are a form of management control, as is organizational control. But technical controls are not management controls. This section is mixing these, and the section heading is “Electronic Access Controls” which are a form of Technical control. What is “external interactive logical access”? If the standard wishes to be prescriptive about procedural controls or technical controls in order to ensure authenticity, then it should be clear about which applies and place them in the proper section accordingly.</p> <p>BPA Transmission is in agreement with the WECC EMS WG’s comments: Strong is a subjective term and needs to be clearly defined. Suggest simply removing the subjective word “strong”.</p> <p>Add “where equipment supports banners” to the end of the last sentence to read “...use banner upon interactive access attempts, where equipment supports banners.” Or reword as follows: "Where technically possible, electronic access control devices shall display an appropriate use banner upon interactive access attempts."</p>	<p>Access points to the perimeter cannot reside within the perimeter.</p> <p>The standard includes access control measures at the access points to the perimeter.</p> <p>1304.a The language in the standard correctly identifies the requirement.</p> <p>There is no assumption made on the nature of the communication links .Intermediate communication transport equipment is not considered as an end-point.</p> <p>1304.a.2 The standard does not require any specific implementation to satisfy these requirements. A control can consist of any combination of people, processes and technical measures necessary to satisfy these requirements.</p> <p>External interactive logical access” implies that access is requested interactively (by a person) by an entity outside of the perimeter. In these cases, strong procedural and/or technical measures are required to ensure authenticity.</p> <p>The term “strong” is used to indicate that measures must be implemented which augment or replace static userid and password authentication. Such measures may include technical solutions such as hardware tokens or digital certificates, or procedural measures such as additional out of band verification before access is enabled. This section of the standard will be amended to clarify the requirement.</p> <p>The standard will include a technical feasibility clause.</p>

Name	Company	Comments	Drafting Team Responses
Tom Flowers	Centerpoint Energy	<p>Page 17, 1304 Electronic Security</p> <p>General comment:</p> <p>The Levels of Noncompliance should refer to “insufficient evidence to support” or “ there is evidence to indicate”.</p> <p>Specific Comments:</p> <p>Page 17, Introduction</p> <p>Replace the paragraph with.... “The responsible entity must create/identify all electronic security perimeters, implement necessary access controls through these perimeters, monitor access into and usage within the perimeter, and have an appropriate level of documentation to support a compliance audit.”</p> <p>Page17, (a)(2) Requirements – Electronic Access Controls</p> <p>Replace the second paragraph with ....”Where technically feasible, all computer monitors through which electronic access is controlled shall display an appropriate use banner upon interactive access attempts.</p>	<p>Page 17, 1304 Electronic Security</p> <p>General comment:</p> <p>The Levels of Noncompliance should refer to “insufficient evidence to support” or “ there is evidence to indicate”.</p> <p>A context for the comment cannot be found in this section.</p> <p>A context for this general comment cannot be found in this section.</p> <p>Page 17, Introduction The overview adequately provides an introduction to the section.</p> <p>Page17, (a)(2) Requirements – Electronic Access Controls, The language in the standard adequately addresses this comment. The requirement will include a technical feasibility clause.</p>

Name	Company	Comments	Drafting Team Responses
Tom Pruitt	Duke Energy	<p>1304 What is the significance of the answer to FAQ#3? There is confusion over how this applies – see comment to section 1302 above.</p> <p>1304(a)(2) “READ ONLY” access should require less control than “USER” or “ADMINISTRATOR” access. Such read only access would be used by maintenance or engineering for troubleshooting, trending, etc. Older systems do not have this ability. For systems that are accessed only through a “client” connection, does the LAN banner displayed at logon to the LAN suffice?</p> <p>1304(b)(3) 90 days is more realistic than previous timeframes.</p> <p>1304, pg 17 Suggestion: please clarify that “control access” can be generic, such as access by anyone via TCP/IP port 25, and that this access control is not only meant to be access by specified users.</p>	<p>FAQ.#3 is intended to clarify situations where administrative dial-up access is provided to a stand-alone critical cyber asset running a non-routable protocol.</p> <p>1304(a)(2) The standard addresses access to the perimeter, not at the application or system level.</p> <p>The standard will include a technical feasibility clause. In the case of access through a client application, the LAN banner displayed at log on will satisfy this requirement.</p> <p>1304(b)(3) 90 days is more realistic than previous timeframes.</p> <p>1304, pg 17 The introductory section is intended as an overview and the current wording adequately summarizes the intent of this section.</p>

Name	Company	Comments	Drafting Team Responses
Tony Eddleman	NPPD	<p>1304(a)(2) Electronic Access Controls: Define "strong" procedural or technical measures.</p> <p>Section 1304(a)(3) needs clarification. What are the expectations for a response to an unauthorized access attempt? Do we need a 24 hour - seven days a week desk watching for events? This will be very expensive for a minimal benefit. Can we use an intrusion detection system (IDS) that sends a page and alerts us? An IDS for all critical cyber assets will be expensive to install and maintain. Is a review of logs every business day sufficient to meet the standard? What is the incident review response time frame?</p>	<p>In section 1304 of the FAQ document, the response to Question 5 explains what is meant by strong authentication with examples. This section and the FAQ will be amended to clarify the requirement.</p> <p>The standard requires only that adequate measures are implemented for monitoring authorized and unauthorized access attempts and to report and alert on unauthorized access attempts. The frequency and timeliness of the alert reviews is determined by the entity's incident response procedures and based on the risk analysis of the cyber assets.</p>

Name	Company	Comments	Drafting Team Responses
William Smith	Allegheny Energy	<p>1304 Electronic Security</p> <p>Clarification is needed in this section as to whether it applies to just access to the security perimeter, such as through a firewall, or whether it also includes all human and electronic access such as user consoles.</p> <p>1304 bullet 1,2 - "All access points" should be "all electronic perimeter access points."</p> <p>1304(b)(2) - The second sentence is confusing and should be broken into bullets or other clear separation of the documentation requirements.</p> <p>1304(a)(1) - "Communications links connecting discrete electronic perimeters are not..." These should be considered as separate critical cyber assets if the data can be intercepted and modified in such a way to cause disturbances. Should encryption and access protection of such connecting data streams be addressed by this standard?</p>	<p>1304 This section will be reviewed for clarity.</p> <p>1304(b)(2) - This section of the standard will be reformatted to clarify the measure.</p> <p>1304(a)(1) - Communication links and in transit encryption are not within the scope of this standard.</p>

# Section 1305 Comments and Drafting Team Responses

Name	Company	Comments	Drafting Team Responses
A. Ralph Rufrano	NYPA	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            --The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            --The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            --The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p>	<p>The Preamble has been modified.</p> <p>1305 a.1 has been modified as suggested.</p> <p>Requirements:            (a)(3) words have been added: "industry or government generally accepted risk assessment methodology            (a)(4) , (5), and (6) The suggested amendments dilute the intent of the requirements.</p> <p>Measures: The drafting team's language has been retained.</p>

Name	Company	Comments	Drafting Team Responses
		<p>"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods.</p> <p>CCTV Video surveillance that captures and records images of activity in or around the secure perimeter.</p> <p>Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Allen Berman	LIPA	<p>1305 Physical Security</p> <p>Introduction 1st bullet Comment: Please clarify what is meant by "an in-depth defense strategy to protect the physical perimeter ".</p> <p>(b) Measures (4) Comment: Does this mean that access points with physical access controls (i.e. card key control) also need "CCTV" or "Alarm Systems"?</p> <p>Comment: Under Alarm Systems, "These alarms must report back to a central security monitoring station or to an EMS dispatcher." Please define an EMS dispatcher.</p> <p>(b) Measures (5) Comment: Must all escorted visitors be logged in one of these manners as part of this standard?</p> <p>(b) Measures (6) Comment: Suggest changing the following sentence from: "The responsible entity shall maintain documentation of annual maintenance and testing for a period of one year. to "The responsible entity shall perform and document maintenance and testing on physical security systems annually. This documentation shall be maintained for a period of one year."</p> <p>(e) Levels of Noncompliance (1) Level One (ii) How do you expect to determine and/or quantify gaps in access records for manual logs?</p>	<p>Introduction 1st bullet Reference to in-depth have been deleted.</p> <p>(b) Measures (4) A new FAQ has been added to address this question.</p> <p>Under Alarm Systems, the words have been changed to read "to a central monitoring station".</p> <p>(b) Measures (5) All escorted visitors must be logged in one of these manners</p> <p>(6) The measure has been modified as suggested.</p> <p>(e) Levels of Noncompliance (1) Level One (ii) has been clarified by the addition of the words "interruptions in system availability" and "in the access records" was removed. The intent is to assess system availability as opposed to gaps in the record.</p>



Name	Company	Comments	Drafting Team Responses
Charles Yeung	SPP	<p>1305 (b) (1) Documentation Review and Maintenance: 90 days to update the physical security plan following a modification to the perimeter or physical security methods is excessive. Maximum of 30 days is recommended.</p> <p>1305 (b) (4) Monitoring Physical Access Control: Is the expectation of this requirement that physical intrusions be prevented, or merely captured "on tape" for later use if an incident occurs? If CCTV is the only methodology used for physical access monitoring, should there be an expectation of real-time human monitoring?</p>	<p>1305 (b) (1) The Drafting Team believes 90 days is consistent with the rest of the standard.</p> <p>1305 (b) (4) Monitoring Physical Access Control: There is no expectation that this be used for real-time prevention but more as a deterrent. See 1305 (a)(4) and 1307 (a)(1) regarding incident response.</p>

Name	Company	Comments	Drafting Team Responses
Charlie Salamone	NSTAR	1305.a.1 - Change "above" to "following"	1305.a.1 The standard has been modified.
		1305.a.6 - Further clarification around "Comprehensive Testing Program"	1305.a.6 - Reference to comprehensive has been removed. The rigor of the program will be measured in the compliance section.

Name	Company	Comments	Drafting Team Responses
Chris deGraffenried	NYPA	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            * The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            * The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            * The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Dave McCoy	Great Plains Energy	<p>1305 - Standard 1305 requires implementation of the necessary measures to control access points to the perimeter(s) and the critical assets within them. This appears to require utilities to put cameras or door alarms on every doorway through which people gain access to locations inside the physical security perimeter. It seems that monitoring a gate at a fenced facility such as a power plant would be sufficient.</p> <p>1305 - Under Measures under Logging Physical Access it is stated that physical access logs shall be retained for at least 90 days. It seems that 30 days should be adequate for videotapes.</p>	<p>The suggestion does not meet the intent of 1305(a)(2) though it could contribute to an improved security strategy. Cyber assets are generally housed inside walled facilities and these are to be secured according to the standard.</p> <p>Measures: The Drafting Team believes 90 days is consistent with the rest of the standard.</p>

Name	Company	Comments	Drafting Team Responses
Dave Norton	Entergy Transmission	<p>Page 22 - 1305 (a) (1) change "their plan" and "their physical..." to "its plan" and "its physical..." ---same comment change "their" to "its" at the top of page 23 (1)</p> <p>Pages 23 &amp; 24 - Please define the following that are used in the standard: "Four Wall Boundary" in quotes on page 23 and not in quotes on page 24, "man trap" on page 23, "access points," "CCTV" on pages 23 &amp; 24, "ESISAC" "ES-ISAC" with a dash, "IAW," and the scope of the new buzzword "malware."</p> <p>Page 23 - (4) second row of the box "...must report back to a central security monitoring station or to an EMS dispatcher." These two options do not apply to all situations. Note also that "EMS dispatcher" is not defined. It seems to refer to someone having control of the EMS software, rather than an operator using EMS software, hardware and databases. And I don't think that was the intent.</p> <p>Page 24 - (b) (5) "Physical access logs shall be retained for at least 90 days..." then in (d) (2) it says "The responsible entity shall keep document revisions and exception and other security event related data including unauthorized access reports for three calendar years. The compliance monitor shall keep audit records for 90 days."</p> <p>Page 24 - The second quote in the question immediately above this mentions document revisions and exception... What exception is allowed? Neither a discussion of exceptions nor a discussion on the authority to make exceptions appear in draft standard 1305.</p> <p>Page 24 - 90 day retention of the access logs and of the audit logs both seem too short. Wouldn't an investigator want to look back further than 90 days if an unauthorized entry were made to see if the same individuals had previously entered, and to learn when and where they entered? Also note that in non-compliance (1) Level One (ii) the standard says "...logging exists but aggregate gaps over the calendar year in the access records exists for a total of less than seven days." Similarly, longer aggregate gaps are the basis for the more serious non-compliance levels two and three. If logs are kept for only 90days, then it seems unlikely that anyone can review a year's worth of logs.</p>	<p>Grammar has been corrected and will be modified for clarity.</p> <p>Page 23 - (4) Reference to EMS Dispatcher has been removed.</p>

Name	Company	Comments	Drafting Team Responses
David Kiguel	Hydro One	<p>Replace 1305 a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.</p> <ul style="list-style-type: none"> <li>- The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),</li> <li>- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and</li> <li>- The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.</li> </ul> <p>-----</p> <p>In 1305 Physical Security, Change the following - (a) Requirements</p> <p>(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.</p> <p>(5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.</p> <p>to</p> <p>(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) We recommend deleting this bullet as the intent is captured in bullet "4".</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.</p> <p>Measures Change</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors.</p> <p>to</p> <p>The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.</p> <p>----- -----</p> <p>1305 Physical Security</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p>	



Name	Company	Comments	Drafting Team Responses
David Little	Nova Scotia Power	<p>305 Physical Security; Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.</p> <ul style="list-style-type: none"> <li>- The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),</li> <li>- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and</li> <li>- The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.</li> </ul> <p>Change the following - (a) Requirements;</p> <p>(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.</p> <p>(5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.</p> <p>to</p> <p>(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity.</p> <p>Change Measures;</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods.</p> <p>CCTV Video surveillance that captures and records images of activity in or around the secure perimeter.</p> <p>Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors.</p> <p>to</p> <p>The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.( the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	<p>1305</p> <p>(2) Physical Security Perimeter: The responsible entity shall identify in its physical security plan the physical security perimeter(s) surrounding its critical cyber asset(s) and all access points to the perimeter(s). Access points to the physical security perimeter(s) shall include all points of physical ingress or egress through the nearest physically secured "four wall boundary" surrounding the critical cyber asset(s).</p> <p>- Unless covered elsewhere, this perimeter may need to be expanded to cover support equipment, such as engine/generator sets, UPS equipment, fire protection equipment and controls, security and card-key controllers, telephone and communication systems, and HVAC systems. Breaching these systems may prove easier for an adversary and yield results as severe as a direct attack upon the cyber asset (or facilitate a more direct attack).</p>	<p>These are dependencies that would be identified in a risk-based threat assessment methodology proposed by the standard.</p>

Name	Company	Comments	Drafting Team Repsonses
Dennis Kalma	AESO	1305.a.2 Should the standard refer to the remaining two sides not referred to here, i.e.: the roof and the floor?	Changed to 6-wall and FAQ added.

Name	Company	Comments	Drafting Team Responses
Ed Goff	Progress Energy	<p>1305 Physical Security</p> <p>The costs associated with these requirements seem significant. Depending on the implementation plan there will be budgetary implications.</p> <ul style="list-style-type: none"> <li>- Items appearing under MEASURES appear to be REQUIREMENTS and should be moved to the appropriate section accordingly.</li> <li>- b.4 - Alarms systems states that alarms must report back to central security monitoring or to an EMS dispatcher... suggest removing reference to EMS dispatcher. Given the broad scope of this standard and assets it includes, there is potential for too many alarms to now be directed to EMS dispatchers. This in itself seems to have the potential for impacting power system reliability in that this creates additional alarm distractions for EMS dispatchers to process</li> </ul>	<ul style="list-style-type: none"> <li>- An implementation plan will be posted with draft version 2 of the standard.</li> <li>- The requirements explain what must be done, and the measures explain how the requirement is to be met. These sections will be reviewed for consistency.</li> <li>- Reference to EMS dispatcher has been removed.</li> </ul>

Name	Company	Comments	Drafting Team Responses
Ed Stein	FirstEnergy	<p>While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.</p> <p>ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.</p> <p>Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.</p> <p>Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide -- Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.</p>	<p>The standard identifies minimums that would meet the security requirement.</p> <p>This standard is intended to protect critical cyber assets. These assets are defined by individual entities using their own risk-based assessment methodologies. The diversity of applicable entities and the cyber assets they identify as critical make it impractical to attempt to do an international financial impact.</p> <p>The team seeks clarification and evidence of where the document refers to the need for many controls such as CCTV in manned facilities. The standard proposes controls around critical cyber assets which will lead to their adequate protection.</p> <p>Page 24 (6) The drafting team believes that a 1 year retention period is reasonable.</p>

Name	Company	Comments	Drafting Team Responses
Ernst Everett	OGE	<p>Section 1305 - Access control needs are different at attended and unattended facilities. Attended facilities do not need alarms in addition to access controls. Some substations may not need access monitoring in addition to access controls, only a policy to report in to a central location.(Possibly substations w/o breakers or SCADA on a blackstart route) Leeway needs to be given to match the controls/monitoring to the needs.</p> <p>Section 1305 - Observed log in is not practical at unattended substations. A logbook along with check in to a central location should be sufficient.</p>	<p>Access control differentiation occurs through the threat/risk/vulnerability assessment.</p> <p>The intent of 1305 is to create a system of conclusive logging at sites containing critical cyber assets. If you believe that a logbook would be unequivocally used, then this is satisfactory, although the drafting team does not.</p>

Name	Company	Comments	Drafting Team Responses
Francis Flynn	National Grid	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305.a.1 with Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.</p> <ul style="list-style-type: none"> <li>- The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),</li> <li>- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and</li> <li>- The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets.</li> </ul> <p>Change the following - (a) Requirements;</p> <p>"(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.</p> <p>(5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall implement the</p>	Please see responses to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Responses
		<p>organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (National Grid recommends deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods.</p> <p>CCTV Video surveillance that captures and records images of activity in or around the secure perimeter.</p> <p>Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility."</p>	

Name	Company	Comments	Drafting Team Responses
Gary Campbell		<p>Measures</p> <p>Items 3,4,5 where the types of access and access controls are specified, these items should be in requirements specified as acceptable methods to complete the requirement in my opinion.</p> <p>Compliance monitoring Process</p> <p>What is the reasoning for the CM keeping audit records for 90 days? The only record the CM should keep is if the entity passed or failed and any mitigation plans associated with non-compliance.</p> <p>Levels of compliance</p> <p>Level 1</p> <p>How does the CM know the known changes? As level 3 (i) has been written, this would be more appropriate.</p>	<p>The NERC standards format calls for a requirements section which identifies the security requirement whereas the measures section explains how the requirement can be met. Team felt that the current layout meets this format..</p> <p>Compliance monitoring Process</p> <p>The only record the CM should keep is documentation as to whether the entity passed or failed and any mitigation plans associated with non-compliance.</p> <p>The wording was changed to "the responsible entity shall keep audit records for 90 days.</p> <p>Levels of compliance Level 1</p> <p>Verbiage has been changed as suggested.</p>

Name	Company	Comments	Drafting Team Responses
Guy Zito	NPCC	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            - The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            - The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            - The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Hein Gerber	British Columbia Transmission Corp.	1305 Physical Security Paragraph (b)(5) requires under Manual Logging that log book or sign-in be accompanied by human observation. Should a critical cyber asset be located at an unmanned site, does this imply that either Computerized Logging or Video Recording will be required?	Yes.

Name	Company	Comments	Drafting Team Repsonses
Howard Ruff	WE Energies	Standard 1305. Regarding "an in-depth defense strategy to protect the physical perimeter", what's considered "in-depth"?	Reference to in-depth has been removed.

Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>1305 Physical Perimeter</p> <p>While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.</p> <p>ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.</p> <p>Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.</p> <p>Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide -- Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.</p>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Repsonses
Joe Weiss	KEMA	Should refer to six-wall boundaries for physical protection, not four-wall (reference appears twice)	Reference has been changed.



Name	Company	Comments	Drafting Team Responses
John Blazeovitch	Exelon	<p>1305.b.3 The term security cage is too restrictive and leaves little room for alternatives. We recommend that security cage be changed to internal perimeter and use security cage as an example.</p> <p>1305.b.3 In the paragraph following the table, the term de-authorization is used. To be consistent with other sections of this standard, we recommend changing de-authorization to revocation.</p>	<p>Security cage has been changed to security enclosure, so as not to limit the type of device to be used.</p> <p>De-authorization has been changed to revocation.</p>

Name	Company	Comments	Drafting Team Responses
John Hobbick	Consumers Energy	<p>1305 Physical Security It should be stated that this section only applies to locations that use routable protocols.</p> <p>Section 1305, first paragraph (following the 3 bullets) discusses the assignment of different security levels for the physical perimeter(s), yet fails to note how these different levels might result in different security requirements.</p> <p>2) Physical Security Perimeter Need to differentiate between the differences of physical security of the computer/control rooms and the substations/plants.</p>	<p>This distinction is made in 1302.</p> <p>Section 1305, first paragraph References to assignment of different security levels have been removed.</p> <p>2) Physical Security Perimeter This differentiation will come as a result of a risk-based threat assessment of all the individual entities' cyber assets. It will vary according to their criticality as determined by each entity.</p>

<b>Name</b>	<b>Company</b>	<b>Comments</b>	<b>Drafting Team Repsonses</b>
Karl Tammer	ISO-RTO Council	1305.b.3 "man trap" should be "Man-trap	This change has been made.

Name	Company	Comments	Drafting Team Responses
Kathleen Goodman	ISO-NE	<p>1305 Preamble</p> <p>Second bullet should explicitly state "Critical Cyber Asset"</p> <p>Throughout 1305, the use of tables, lists, and examples is both confusing and too restrictive. As a standard, if those are the only identified, then other equitable solutions are not allowed by exclusion. Remove all tables, lists, and examples, to allow appropriate risk management decisions.</p> <p>1305 Measures:</p> <p>(4) Should not report back to the EMS Dispatcher. The primary functions of our system operators should not be impaired by requiring them to be security guards, as we have all learned all too well in the blackout, a power system degrade and collapse can happen within seconds. Their job is grid reliability, not manage cyber security.</p> <p>(5) Do not mandate all these logs. The Logs required should be consistent with the risk assessment based solution implemented.</p> <p>1305 Levels Noncompliance</p> <p>(2.i) Strikeout reviewed last six months. Requirement is for 90 day update, annual review.</p>	<p>Bullet was removed.</p> <p>Measures:</p> <p>(4) Reference to EMS dispatcher has been removed.</p> <p>(5) The requirement is to implement one of the methods. The drafting team does not believe the requirement would cause inconsistency with solutions determined as a result of a risk assessment.</p> <p>Levels Noncompliance</p> <p>Timeframes will be for consistency.</p>

Name	Company	Comments	Drafting Team Responses
Ken Goldsmith	Alliant Energy	<p>1305 Physical Security</p> <p>Levels of non-compliance in this section are inconsistent with 1306.</p> <p>Article b-4 Change Alarm Systems to be Access Control System.</p> <p>Article b-5 If the only method used for logging physical access is video, unable to meet 90-day retention with digital video systems.</p>	<p>Levels of noncompliance will be reviewed for consistency.</p> <p>The term alarm systems are more compatible with this section, which refers to monitoring.</p> <p>Article b-5 A 90 retention of digital video systems is feasible. See FAQ.</p>

Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	<p>Section 1305</p> <p>(a)(2) -- Reference to "the nearest secured 'four wall boundary'" is overly prescriptive and duplicative, or at least needs to be clarified and/or limited to appropriate facilities. For instance, multiple layers of security already exist generally for attended facilities such as generating plants (e.g., outer perimeter screening and other measures similar to Section 1305[b]). Of particular concern is the extreme difficulty (both in time and money) involved with preventing "surfing" or "tailgating," especially at unattended facilities. Similar difficulties are attendant upon attempts to monitor all egress.</p> <p>(b)(3)(table)(4th item) -- This is too restrictive a definition -- consider changing the name from "Security Cage" to "Additional Perimeter" or "Internal Perimeter." In any event, change the definition to read: "An additional, internal secured perimeter within a secured area that permits additional control of physical access to a cyber asset within a larger (usually secured) perimeter, such as by means of a 'cage' or cabinet."</p> <p>(b)(3)(text)(2nd parag.) --</p> <p>The phrase "documentation [re implementation] for each physical access point" will lead to far too much paperwork for numerous, identical physical access points. Where there are several identical or substantially equivalent access points for one or a group of security perimeters, this language should be interpreted as requiring only records indicating the controls implemented for the type of access point, and the location of each such individual point. It would be better to change the language to read: "for all physical access points."</p> <p>The term "de-authorization" is unclear -- change to "revocation."</p> <p>(b)(4)(table)(2nd item) -- The wording implies that an audible or visual alarm must go off at every access. This would lead users to turn off or ignore the alarm. Only unauthorized or forced access events should be alarmed. This item should be revised to read as follows:</p> <p>"Access Control System" -- "A system that logs and records each access event, including those of unauthorized or forced entry (which must give rise to an alarm). When an alarm is appropriate, the alarm system must be based on" [REMAINDER OF TEXT AS IN ORIGINALLY PROPOSED DRAFT].</p>	<p>(a)(2) Rreference was changed to "six-wall boundary". The drafting team recognizes that tailgating is a common vulnerability and believes it is best addressed in employee awareness sessions. The solution of large turn-styles is effective but costly.</p> <p>(b)(3)(table)(4th item) Security cage has been changed to security enclosure, which does not limit the type of device to be used.</p> <p>(b)(3)(text)(2nd parag. Verbiage has been changes as suggested.</p> <p>(b)(4)(table)(2nd item) The drafting team believes the existing language conveys the correct intent.</p> <p>(b)(5)(table)(1st item) Added "remote verification"</p>

Name	Company	Comments	Drafting Team Responses
		(b)(5)(table)(1st item) -- Manual logging will be difficult or impossible at unmanned locations, and is not even required by the NRC at all locations. Moreover, for safety reasons, access to unmanned substations must be reported by phone, etc., in almost all circumstances. The supporting text should be modified to read: "A log book or sign-in sheet or other record of physical access accompanied by remote verification."	

Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>1305 -- Physical Perimeter</p> <p>While Cinergy acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.</p> <p>Cinergy's interpretation of current draft language in Section 1302 will result in almost all Cinergy generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. Cinergy believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. Cinergy recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.</p> <p>Generating plants control rooms may be manned 24 hours a day seven days a week. Cinergy seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.</p> <p>Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide -- Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.</p>	Please see responses to Ed Stein.



Name	Company	Comments	Drafting Team Responses
Linda Campbell	FRCC	<p>1305 Physical Security</p> <p>It is not clear why "different security levels shall be assigned" and what difference the security levels would make in implementing the requirements in this standard. The Q&amp;A in this section #4 indicates the organization may establish higher levels. Seems like it should be optional -- shall doesn't sound optional.</p> <p>(a) Requirements</p> <p>(a) (1) Requirement #1 appears to be in the wrong location (should be last since it references the above requirements?).</p> <p>(a) (2) Can the nearest "4 wall boundaries" be defined as a cage or a locked cabinet ? Securing a substation control house to provide a physical security perimeter is a problem. Many people need access to the control house for routine work. However, there may only be one or two racks of equipment that are defined as a "Critical Cyber Asset". We need to secure those assets (RTU, router, etc) without causing unnecessary hindrances to routine substation operation.</p> <p>Complying with these requirements as written will also be very difficult, costly and dangerous for our generating stations. The control rooms are centers of activity with the operations personnel monitoring and approving all activities occurring on-site. On most days this includes hundreds of contractors that must come to the control room to get HEC tagging, Hot Work or Confined Space Entry Permits approved. The short term nature of the most contractor employees is such that maintaining lists and background screening of all is nearly impossible. If we create another area for this activity, then operations may not be able to monitor what all is taking place causing operational and safety issues that may impact reliability. Creating another area for this activity would also require the stations to hire additional employees to cover this location 24/7 (5 people per station).</p> <p>(a) (5) recommend changing "technical and procedural mechanisms" to "technical or procedural mechanisms"</p> <p>(b) Measures</p> <p>(b) (1) Recommend changing "physical security methods" to "physical access controls" and moving this measure to the bottom of the measures.</p> <p>(b) (4) Add "Human monitoring or observation: to the</p>	<p>Reference to different security levels has been removed.</p> <p>Requirements</p> <p>(a) (1) Text changed to "following requirements"</p> <p>(a) (2))Yes. It will be up to each entity to define its security perimeter according to the threat and criticality of the asset. This may be 6 walls or a security enclosure or some other mechanism that meets the intent of the standard.</p> <p>(a) (5) The standard only applies to personnel who access critical cyber assets, not everyone. Knowing who has access is intended to help protect those assets. An effective system of personnel identification must be applied and additional rigor must be applied to defining security perimeters in the interest of operational efficiency.</p> <p>The drafting team believes both are required, ie: Technical mechanisms *and* procedures around these mechanisms.</p> <p>Measures</p> <p>(b) (1) The drafting team believes its terminology is more encompassing and more effective.</p> <p>(b) (4) Wording was changed to "remote verification"</p> <p>(d) (2) keep document revisions and exceptions and other security – requirements don't mention exceptions.</p> <p>(d) (3) (ii) The section has been modified include Configuration documents.</p> <p>(e) and (e) (1,2,3) (ii) Timeframes will be reviewed for consistency.</p>

Name	Company	Comments	Drafting Team Responses
		monitoring methods	
		(d) (2) keep document revisions and exceptions and other security -- requirements don't mention exceptions.	
		(d) (3) (ii) -- Documents for configuration, processes, etc. Configuration not mentioned in the requirements.	
		(e) The levels of non-compliance within this section and those within section 1304 should be more consistent with each other. This section specifies 1 week at level 1, one month at level 2 and 90 days at level 3, while 1304 is one week, less than one day, and less than one week at the same levels. Also the numbered references don't exist in the document.	
		(e) (1,2,3) (ii) Log retention is required for 90 days, but the non-compliance sections addresses gaps over a 1 year period. If the logs are retained for only 90 days how can you evaluate over a 1 year period?	

Name	Company	Comments	Drafting Team Responses
Lyman Schaeffer	Pacific Gas & Electric	<p data-bbox="590 164 821 188">1305 Physical Security:</p> <p data-bbox="590 220 1209 355">The proposals here are consistent with the direction the industry is moving. Our concern is the time frame to have such measures in place as the costs and time to engineer and construct physical security measures can be tremendous particularly for a company with multiple bulk power substations.</p>	<p data-bbox="1245 164 1759 220">A draft implementation plan will be posted with draft version 2 of this standard.</p>

Name	Company	Comments	Drafting Team Responses
Michael Anderson	Midwest ISO	<p>Physical Security</p> <p>Can the requirement for physical security logging be expanded? Specifically can the section on video logging be expanded?</p> <p>Logical Security Assessment/Physical Security - Why is the assessment requirement specifically described for logical security but not for physical security? Can this item be addressed with equal diligence?</p>	<p>Unclear as to intent of comment.</p> <p>See a (2) for reference to risk-based assessment methodology.</p>

Name	Company	Comments	Drafting Team Responses
Neil Phinney	Georgia Transmission Co	<p>1305.b.3 This would appear to prohibit common locks on substations. "Special locks" are not adequately defined, but it would appear that a standard key lock would not suffice.</p> <p>1305.b.5 This appears to prohibit our current process of remotely logging in our control center the access to substations because it would not be "accompanied by human observation"</p>	<p>1305.b.3 The intent is to apply two mechanisms to critical cyber assets: locking and logging. Both these features are present in card key systems. However, this does not preclude using standard locks with other logging mechanisms.</p> <p>1305.b.5 Text was changed to add "remote verification."</p>

Name	Company	Comments	Drafting Team Responses
Paul McClay	Tampa Electric Company	<p>1305 Physical Security</p> <p>It is not clear why "different security levels shall be assigned" and what difference the security levels would make in implementing the requirements in this standard. The Q&amp;A in this section #4 indicates the organization may establish higher levels. Seems like it should be optional -- shall doesn't sound optional.</p> <p>(a) Requirements</p> <p>(a) (1) Requirement #1 appears to be in the wrong location (should be last since it references the above requirements?).</p> <p>(a) (2) Can the nearest "4 wall boundaries" be defined as a cage or a locked cabinet ? If not consider changing this to "It is defined as the nearest physical boundary that can be physically secured..."</p> <p>Securing a substation control house to provide a physical security perimeter is a problem. Many people need access to the control house for routine work. However, there may only be one or two racks of equipment that are defined as a "Critical Cyber Asset". We need to secure those assets (RTU, router, etc) without causing unnecessary hindrances to routine substation operation.</p> <p>Complying with these requirements as written will also be very difficult, costly and dangerous for our generating stations. The control rooms are centers of activity with the operations personnel monitoring and approving all activities occurring on-site. On most days this includes hundreds of contractors that must come to the control room to get HEC tagging, Hot Work or Confined Space Entry Permits approved. The short term nature of the most contractor employees is such that maintaining lists and background screening of all is nearly impossible. If we create another area for this activity, then operations may not be able to monitor what all is taking place causing operational and safety issues that may impact reliability. Creating another area for this activity would also require the stations to hire additional employees to cover this location 24/7 (5 people per station).</p> <p>(a) (5) recommend changing "technical and procedural mechanisms" to "technical or procedural mechanisms"</p> <p>(b) Measures</p> <p>(b) (1) Recommend changing "physical security methods" to "physical access controls" and moving this measure to the</p>	<p>Reference to different security levels has been removed.</p> <p>Requirements</p> <p>(a) (1) Text changed to "following requirements"</p> <p>(a) (2))Yes. It will be up to each entity to define its security perimeter according to the threat and criticality of the asset. This may be 6 walls or a security enclosure or some other mechanism that meets the intent of the standard.</p> <p>(a) (5) The standard only applies to personnel who access critical cyber assets, not everyone. Knowing who has access is intended to help protect those assets. An effective system of personnel identification must be applied and additional rigor must be applied to defining security perimeters in the interest of operational efficiency.</p> <p>The drafting team believes both are required, ie: Technical mechanisms *and* procedures around these mechanisms.</p> <p>Measures</p> <p>(b) (1) The drafting team believes its terminology is more encompassing and more effective.</p> <p>(b) (4) Wording was changed to "remote verification" Your understanding is correct, except that logging still applies. Therefore, people who are escorted "at all times" are exempt for all but logging physical access. The team produced an FAQ from this comment.</p> <p>(d) (2) keep document revisions and exceptions and other security – requirements don't mention exceptions.</p> <p>(d) (3) (ii) The section has been modified include Configuration documents.</p> <p>(e) and (e) (1,2,3) (ii) Timeframes will be reviewed for consistency.</p>

Name	Company	Comments	Drafting Team Responses
		bottom of the measures.	
		(b) (4) Add "Human monitoring or observation: to the monitoring methods	
		Based on our previous suggestions re "escorted access", it is our understanding that: "By virtue of a room containing critical cyber asset(s) being staffed at all times, 24 hours per day, 7 days per week, personnel who enter these rooms are given "escorted" or "restricted" access as long as there is a formal shift handoff between authorized personnel and the room is capable of being secured in case of an emergency evacuation. . Thus personnel entering these rooms are exempted from the requirements for background checking, training, and logging physical access. Is this a correct interpretation?	
		(d) (2) keep document revisions and exceptions and other security -- requirements don't mention exceptions.	
		(d) (3) (ii) Documents for configuration, processes, etc. Configuration not mentioned in the requirements.	
		(e) The levels of non-compliance within this section and those within section 1304 should be more consistent with each other. This section specifies 1 week at level 1, one month at level 2 and 90 days at level 3, while 1304 is one week, less than one day, and less than one week at the same levels. Also the numbered references don't exist in the document.	
		(e) (1,2,3) (ii) Log retention is required for 90 days, but the non-compliance sections addresses gaps over a 1 year period. If the logs are retained for only 90 days how can you evaluate over a 1 year period?	

Name	Company	Comments	Drafting Team Repsonses
Pedro Modia	FPL	[Further clarification is required in regards to "investigations upon complaint." How intrusive are these investigation, and what would predicate such investigations?]	Investigations are part of NERC's Compliance Program.



Name	Company	Comments	Drafting Team Responses
Phil Sobol	SPP CIPWG	1305.b.4 -- "EMS Dispatcher" - How generic or specific is this term? Is this a "certified operator" or an "uncertified operator"? Keep in mind that not only is there an EMS (Energy Management System) but a Distribution Management System (DMS) and a Transmission Management System. It would be better stated in this manner. "These alarms must report back to a monitoring station that is manned on a 24x7x365 basis.	Reference to EMS Dispatcher has been removed.

Name	Company	Comments	Drafting Team Responses
Ray A'Brial	CHGE	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with; Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.</p> <ul style="list-style-type: none"> <li>- The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),</li> <li>- The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and</li> <li>- The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</li> </ul> <p>Change the following - (a) Requirements; "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s). (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week. (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access. (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet 4).</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p>	
		Change Measures;	
		<p>(b)(3)(table)(4th item) -- Too restrictive a definition: consider changing name from Security Cage to Additional Perimeter or Internal Perimeter -- in any event, change the definition to read: An Additional, internal secured perimeter within a secured area that permits additional control of physical access to a cyber asset within a larger (usually secured) perimeter, such as by means of a cage or cabinet.</p>	
		<p>(b)(3)(text)(2nd parag.) -- documentation [re implementation] for each physical access point: Far too much paperwork for numerous, identical physical access points. Where there are several identical or substantially equivalent access points for one or a group of security perimeters, this language should be interpreted as requiring only records indicating the controls implemented for the type of access point, and the location of each such individual point. Better to change the language to read: for all physical access points.</p>	
		<p>(b)(4)(table)(2nd item) -- Wording implies that an audible or visual alarm must go off at every access. This would lead users to turn off or ignore the alarm. Only unauthorized or forced access events should be alarmed. This item should be revised to read as follows:</p> <p>Access Control System -- A system that logs and record each</p>	

Name	Company	Comments	Drafting Team Responses
		<p>access event, including those of unauthorized or forced entry (which must give rise to an alarm. When an alarm is appropriate, the alarm system must be based on" [REMAINDER OF TEXT AS IN ORIGINALLY PROPOSED DRAFT]</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods.  CCTV Video surveillance that captures and records images of activity in  or around the secure perimeter.  Alarm Systems An alarm system based on contact status that indicated a door or  gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors.</p> <p>to</p> <p>The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility.</p> <p>(b)(5)(table)(1st item) -- Manual logging will be difficult or impossible at unmanned locations, and is not even required by the NRC at all locations. Moreover, for safety reasons, access to unmanned substations must be reported by phone, etc., in almost all circumstances. The supporting text should be modified to read: "A log book or sign-in sheet or other record of physical access accompanied by remote verification."</p>	

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p data-bbox="590 164 831 188">1305 Physical Perimeter</p> <p data-bbox="590 220 1209 302">While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.</p> <p data-bbox="590 334 1209 643">ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.</p> <p data-bbox="590 675 1209 781">Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.</p> <p data-bbox="590 813 1209 1062">Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide -- Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.</p>	Please see response to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>1305 --Physical Perimeter</p> <p>While ABC acknowledges that controls may be required, it does not seem appropriate for NERC to dictate the controls to be implemented. Example: Implement CCTV or Alarm System.</p> <p>ABC's interpretation of current draft language in Section 1302 will result in almost all ABC generating plants being subject to these rules. Section 1305 then seeks to name the controls, which must be implemented at each asset location. No mention to a review of costs associated with such sweeping changes is even mentioned in any of the language. ABC believes it is appropriate to address the costs and corresponding benefits before moving forward with such a sweeping and costly initiative. ABC recommends that participants and NERC develop an estimate of the proposed cost to the industry before finalizing these requirements.</p> <p>Generating plants control rooms may be manned 24 hours a day seven days a week. ABC seeks clarification and evidence of the need for the many controls, such as CCTV, which are specified in the document in these cases where facilities are manned.</p> <p>Page 24 (6) Maintenance and testing of security systems to be retained for 1 yr. This involves corp. wide -- Equipment Maintenance area. This is one more example of the costs, which must be considered before moving forward. These types of requirements are very costly to large organization because they impose enterprise wide requirements. Maintenance records on the security installation equipment will not be kept in Electric Operations areas. Requirements will need to be coordinated across groups responsible for equipment maintenance.</p>	Please see responses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Richard Engelbrecht	Rochester Gas & Electric	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            - The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            - The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            - The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	



Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p data-bbox="590 164 1066 185">Clarify Four-wall Boundary in Section 1305.a.2.</p> <p data-bbox="590 220 1150 272">Section 1305: Regarding self-certification, will there be a standard form to complete?</p>	<p data-bbox="1245 164 1759 217">Section 1305.a.2. Four-wall has been replaced by six-wall. Examples have now been provided in an FAQ.</p> <p data-bbox="1245 248 1759 302">The compliance monitor determines the appropriate form.</p>

Name	Company	Comments	Drafting Team Responses
Robert Pelligrini	United Illuminating	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            - The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            - The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Robert Snow		<p data-bbox="590 164 680 188">Physical:</p> <p data-bbox="590 220 1205 329">In locations that are not normally occupied, there should not be documents, prints, systems descriptions or other detailed information that would aid someone understand how the system operates or to bypass the intended safeguards in the system.</p>	Agreed.

Name	Company	Comments	Drafting Team Responses
Robert Strauss	NYSEG	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            - The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            - The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            - The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall</p>	Please see responses to A. Ralph Rufrano

Name	Company	Comments	Drafting Team Responses
		<p>implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter. Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>1305 (Physical Security)</p> <p>-In (e)(1)(2), there is no reasonable lower bound. The standard states any aggregate gap in logs less than seven days is a non-compliance. Is a two-minute gap over a year's time a non-compliance? If I have video-monitoring, just switching tapes makes me non-compliant. If a storm takes down my network communications so that I can't receive door/gate alarms for a few hours, should that require filing non-compliant on a cyber security standard for the year? Some grace period must be allowed.</p> <p>- (1st bullet under opening paragraph) -- change "in depth defense" to "adequate"</p> <p>- (a)(4) Add -- "This may be accomplished through direct (internal personnel monitoring) electronic access controls or cctv."</p> <p>- (a)(6) Change "comprehensive" to "adequate".</p> <p>- (b)(4) Add -- "Facilities which are not staffed with authorized personnel 24/7 should maintain a system which maintains physical access control through intrusion detection devices".</p> <p>- (b)(4)(cctv) - Add "...or point of facility access".</p> <p>- (b)(4) Alarm Systems -- Clarify that an alarm is only required when a door or gate has been unopened without authorization.</p> <p>- (b)(5) change 90 to 30 (many digital video cameras will not record for longer than 30 days before recording over stored data.</p>	<p>(e)(1)(2)Time periods have been clarified.</p> <p>(1st bullet) Referneces to defense in depth have been removed.</p> <p>(a)(4) This verbiage was added.</p> <p>(a)(6) The word comprehensive was removed.</p> <p>(b)(4) In the physical security world, IDD's are called alarm systems.</p> <p>(b)(4)(cctv) - Modified as suggested.</p> <p>(b)(4) the standard has been clarified.</p> <p>(b)(5) The drafting team believes 90 days is feasible. Please see FAQ.</p>

Name	Company	Comments	Drafting Team Responses
S. Kennedy Fell	NYISO	<p>1305 Physical Security;</p> <p>Eliminate the bulleted items in the Preamble to Section 1305- they appear in the Requirement section.</p> <p>Replace 1305 a.1 with;            "Documentation: The responsible entity shall document their implementation of the following requirements in their physical security plan.            - The identification of the physical security perimeter(s) and the development of a defense strategy to protect the physical perimeter within which critical cyber assets reside and all access points to these perimeter(s),            - The implementation of the necessary measures to control access at all access points to the perimeter(s) and the critical cyber assets within them, and            - The implementation of processes, tools and procedures to monitor physical access to the perimeter(s) and the critical cyber assets."</p> <p>Change the following - (a) Requirements;            "(3) Physical Access Controls: The responsible entity shall implement the organizational, operational, and procedural controls to manage physical access at all access points to the physical security perimeter(s).            (4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, technical, and procedural controls, including tools and procedures, for monitoring physical access 24 hours a day, 7 days a week.            (5) Logging physical access: The responsible entity shall implement the technical and procedural mechanisms for logging physical access.            (6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all physical security systems (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>to</p> <p>"(3) Physical Access Controls: The responsible entity shall implement the organizational, and /or operational, and/or procedural controls to manage physical access at all access points to the physical</p>	Please see responses to A. Ralph Rufrano.



Name	Company	Comments	Drafting Team Responses
		<p>security perimeter(s) following a risk assessment procedure.</p> <p>(4) Monitoring Physical Access Control: The responsible entity shall implement the organizational, and/or technical, and/or procedural controls, including tools and procedures, for monitoring implemented physical access controls 24 hours a day, 7 days a week.</p> <p>(5) (We recommend deleting this bullet as the intent is captured in bullet "4").</p> <p>(6) Maintenance and testing: The responsible entity shall implement a comprehensive maintenance and testing program to assure all implemented physical access controls (e.g., door contacts, motion detectors, CCTV, etc.) operate at a threshold to detect unauthorized activity."</p> <p>Change Measures;</p> <p>"(4) Monitoring Physical Access Control: The responsible entity shall implement one or more of the following monitoring methods. CCTV Video surveillance that captures and records images of activity in or around the secure perimeter.</p> <p>Alarm Systems An alarm system based on contact status that indicated a door or gate has been opened. These alarms must report back to a central security monitoring station or to an EMS dispatcher. Examples include door contacts, window contacts, or motion sensors."</p> <p>to</p> <p>"The responsible entity shall implement an appropriate monitoring method consistent with its preferred risk assessment procedure for that specific facility." ( NPCC believes the selection of monitoring should be driven by a risk assessment study and that it is not appropriate to require Video or Alarm Systems especially when they may be unattended.)</p>	

Name	Company	Comments	Drafting Team Responses
Scott McCoy	Xcel Energy	<p>Section 1305, Requirement (1) Documentation section assumes that there is one central security plan for the whole company vs. a security program. If this standard requires a 1300 security plan, then that is what it should say. Otherwise, it should just state that "the company shall have a documented implementation plan approved by the a senior manager responsible for the implementation of NERC 1300.</p> <p>Section 1305, Measures (3) Physical Access Controls. Security cage does not belong in this list it is not interchangeable with the other 5 options. it is the same a walls or a perimeter fence around a sub station, just a smaller application and is covered under "four wall boundary". Also, Specialty Locks are from magnetic locks, which require some type of activation, which is covered under Other Authentication Devices. Mag locks, electric strikes and/or electrified mortise (to name a few) are implied when using a Card Key or Device. If not electric specialized locks are an option, and then it should only state, "Lock sets with restricted key system.</p> <p>Section 1305, Measures (4) Alarm System. The first sentence is not consistent with the rest of the paragraph. "Ana alarm system based on the contact status that indicated a door or gate has been opened". This is consistent with a programmable alarm system which will report the state of a contact, open or shut and hold programming which will initiate an alarm based on a given state. The examples that follow (excluding door contact) are part of an intrusion detection system not related to an open or closed state of a door or gate. What is the goal? Do you want a system capable of reporting the state of a door or gate on the physical perimeter? Do you want to require an additional physical intrusion detection system? I recommend adding a section dealing with intrusion detection from alarm systems to clarify the measure. One or more of the following is not applicable in this measure, the two stated options are not interchangeable, they accomplish things. Either requires a minimum (recommend door state monitoring/reporting) and then one or more of the following (CCTV, Intrusion Detection etc.)</p>	<p>Requirement 1 - A 1300 security plan is not contemplated in this standard. Rather, any existing security plans or programs should be aligned with the 1300 standard.</p> <p>Measures (3) The intent of this section was to offer good examples of adequate security devices for this standard. The intent was to offer guidance to organizations which might not have dedicated security staff.</p> <p>Measures (4) "based on contact status" was removed. This is at the option of the entity. The goal is to create the necessary security perimeter alarm system to meet the standard of protecting critical cyber assets.</p> <p>The drafting team does not believe these requirements are too prescriptive; rather, they define a reasonable level of physical security.</p>

Name	Company	Comments	Drafting Team Responses
Terry Doern	BPA	<p>How do you define and gauge an "in-depth defense strategy"? The statement "When physical perimeters are defined" implies that they may not be defined. However it is earlier stated that defining a "physical security perimeter" is a requirement. This should be resolved.</p> <p>The "different security levels" are vague, and should be tied to an assessment of the residual risk to the critical cyber assets and the impact of their loss or compromise.</p> <p>Suggested text: Physical perimeters shall be defined and where possible, layers of physical security shall be implemented with different security levels to these perimeters depending on the level of criticality of assets within these perimeter(s).</p>	<p>Reference to defense in depth has been removed.</p> <p>Reference to different security levels has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Tom Flowers	Centerpoint Energy	<p>Page 17, 1305 Physical Security General comment: In the Measures subsection, some discussion needs to occur about exit controls. This is not anti-pass back because it doesn't matter how an individual got into the physical security area. Rather it is a form of failure management. For example, if an individual gets into a secure area by accident, tail gating, or malicious means they will not be allowed to exit without a trace that the unauthorized entry ever occurred. This should be discussed in subsection (b)(3).</p> <p>Specific Comments: Page 22, Introduction Replace the paragraph with.... "The responsible entity must create/identify all physical security perimeters, implement necessary access controls through these perimeters, monitor access into and usage within the perimeter, and have an appropriate level of documentation to support a compliance audit."</p> <p>Page 22, (a) Requirements Replace the first paragraph with..."(1) Physical Security Plan: The responsible entity shall develop and maintain a Physical Security Plan for use and application at all of its physical sites containing critical Cyber assets."</p> <p>Insert after the last requirement... "(7) Documentation: The responsible entity shall maintain sufficient documentation concerning its implementation of its Physical Security Plan to support a compliance audit."</p> <p>Page 23, (b)(3) Physical Access Controls Replace "Security Cage" with "Additional Physical Perimeters" in the table. Use the cage as an example.</p> <p>Replace "de-authorization" with "revocation" in the second paragraph. Page 23, (b)(4) Monitoring Physical access Control</p> <p>Replace "Alarm System" with "Access Control System" in the table. Use the open door alarm as an example.</p> <p>Page 24, (b)(5) Logging Physical Access Replace "human observation" with "human observation or remote verification"</p>	<p>The team felt that the safety and practicality issues would be impacted by this type of measure and that it still would not provide conclusive evidence of the departure of an unauthorized person because of emergency egress provisions.</p> <p>Specific Comments: Page 22, Introduction The standard has been modified to refer only to the physical security perimeter within which the cyber assets reside. The focus of this section is on the cyber asset and not the whole security perimeter.</p> <p>Page 22, (a) Requirements Section 1302 identifies which sites need to be secured and this section focus on the techniques for securing them.</p> <p>The words "sufficient to support a compliance audit" were added to this section.</p> <p>Page 23, (b)(3) Physical Access Controls The term security cage was changed to to security enclosure.</p> <p>Replaced "de-authorization" with "revocation" in the second paragraph.</p> <p>Page 23, (b)(4) The drafting team believes alarm system and access control systems are different and has retained the original language.</p> <p>Page 24, (b)(5) Replaced "human observation" with "human observation or remote verification"</p> <p>Page 24, (b)(6)The term appropriate period is too vague.</p>

Name	Company	Comments	Drafting Team Repsonses
		<p>Page 24, (b)(6) Maintenance and Testing of Physical Security Systems:</p> <p>Replace the Paragraph with... "The responsible entity shall maintain documentation of all testing for an appropriate period of time to support a compliance audit."</p>	

Name	Company	Comments	Drafting Team Responses
Tom Pruitt	Duke Energy	<p>1305 This standard could require significant physical security upgrades and tremendous cost depending on types and numbers of facilities to which it would apply.</p> <p>The answer to FAQ#6 is not consistent with measures 3, 4, and 5.</p> <p>1305, pg 24 Using the terms defined in the definitions, suggest that this sentence reads: "The responsible entity shall have a process for creating unauthorized incident access security incident reports."</p>	<p>A risk assessment will narrow the scope of assets that must be physically protected.</p> <p>The standard and FAQs will be revised for consistency.</p> <p>1305, pg 24 Definitions have been revised.</p>

Name	Company	Comments	Drafting Team Responses
William Smith	Allegheny Energy	<p>5. 1305 Physical Security</p> <p>Critical Cyber Assets located in substations and generating stations with a sufficient local electronic security perimeter should not require the physical security perimeter requirements of critical cyber assets. (Refer to comments under Question 2.)</p> <p>Also, anyone with direct physical access to the critical cyber assets in either instance can easily manually control the transmission and generating bulk electric assets.</p> <p>The NERC Security Guideline concerning Substation Physical Security and typical generating physical security provides the guidance and protection required for these assets.</p> <p>Do all remote workstations that access a dial-up enabled critical cyber asset automatically become critical assets themselves?</p> <p>1305(b)(4) - The last two sentences are confusing as to what is being asked for. Not sure what "verify access records for authorized access against access control rights" means as well as "shall have a process for creating unauthorized incident access reports"?</p>	<p>This is correct as long as the existing system meets NERC 1300 requirements. Remember that the focus is on the critical cyber asset.</p> <p>Agreed, but this standard must address physical security of critical cyber assets or their protection would be incomplete.</p> <p>Please refer to 1302 or 1304 for guidance.</p> <p>1305(b)(4) - The sentence was changed to "Additionally, the documentation shall describe the processes to review records for unauthorized access."</p>

# Section 1306 Comments and Drafting Team Responses

Name	Company	Comments	Responses
A. Ralph Rufrano	NYPA	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;  "A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."  to  "A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets."  (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;  "A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."  to</p>	<p>1306.a.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.</p> <p>1306.a.02 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.02.i The drafting team believes the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>The intent was to emphasize there are alternatives which provide more protection than passwords.</p> <p>1306.a.02.ii Noted.</p> <p>1306.a.02.ii The word was chosen to distinguish between (1) vendor created accounts and (2) group accounts versus individually created end user accounts.</p> <p>1306.a.02.ii The drafting team believes a policy would more adequately address this requirement.</p> <p>1306.a.02.iii The drafting team believes reviews should be conducted more frequently than annually.</p> <p>1306.a.03 The drafting team is in agreement with your comment. It is stated this way because not everyone looks at software updates in the same manner.</p> <p>1306.a.03 The intended interpretation of this sentence applies to systems where software updates are not possible, e.g., the Operating System Upgrade or Patch may break the application, In this circumstance, an alternate method of protection must be put in place, e.g., a security appliance is placed inline with the system or it should not be connected to a wide area network with Internet connectivity.</p>



Name	Company	Comments	Responses
		<p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>Change 1306.a.6 from            "All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."            to            "It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".</p> <p>1306.b.3, remove;</p>	<p>1306.a.03 The intent of the standard is to recognize limitations of legacy equipment and the ability to manage the risk with a variety of actions that could avoid upgrades and patches. For example, containing connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.05 Reference to penetration test removed.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using monitoring systems and/or procedures either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine its own logging strategy to fulfill the requirement. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.06 Being highly situation-dependent, the responsible entity must determine its own logging strategy that fulfills the requirement. This strategy must be sufficient to support the investigation of an event, and assure the integrity of these electronic records is maintained. In the unusual instance where in-use equipment does not natively provide appropriate logging capabilities, a reasonable best-effort work-around solution must be implemented. It is not intended that equipment be rendered obsolete out of hand strictly due to this requirement, nor that the responsible entity be held non-compliant where best-effort has been expended to use the native capabilities of the equipment, for the duration of its normal useful life.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal</p>

Name	Company	Comments	Responses
		<p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vendor security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change  ".so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."  to  "..mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;  "Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence.  Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;  "The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured</p>	<p>and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>1306.a.07 The drafting team acknowledges your comments and this topic will be addressed as a governance item covered in section 1301.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage.</p> <p>1306.a.10 This requirement is about "situational awareness" of networked-computing infrastructure. Each responsible entity will have to figure out for itself how it will establish and maintain situational awareness of its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented</p> <p>1306.a.11 The two sections noted talk about different things. 1308 is about disaster recovery and business continuity planning. The backups created as per section 1306, among other things, are used as part of the recovery processes defined in 1308.</p> <p>1306.b.01 Agreed</p> <p>1306.b.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing</p>

Name	Company	Comments	Responses
		from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."	activities.
		to "Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."	1306.b.02 The drafting team agrees and will update the standard accordingly.  1306.b.03 The drafting team wants to emphasize the importance of vulnerability awareness and the need to demonstrate an ongoing awareness and measurable actions to mitigate vulnerabilities.
		1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"	1306.b.03 Agreed, because the word "approved" implies authorization and oversight.
		Remove 1306.b.11, since 1306.a.11 was removed.	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.
		1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."	1306.b.05 The drafting team respectfully disagrees. Outsourcing does not relieve management of fiduciary oversight responsibility
		1306.d.3.iii, change "system log files" to "audit trails"	1306.b.06 The drafting team respectfully disagrees. Logs are the basis for audit trails, and logs record "events." An audit trail can and usually is at least in part comprised of event log data. So, it is event logs that must be retained, to support the audit trail. An audit trail can be thought of as (documentation of) a "control process," part of which consists of event logs.
		1306.e.2, change "the monthly/quarterly reviews" to "the reviews"	
		1306.e.2.ii.C, change "anti-virus" to "malicious"	1306.b.07 Remove all—agreed. The drafting team acknowledges your comments and this topic will be addressed as a governance item covered in section 1301.
		1306, the Compliance levels should be updated to match the above measures.	1306.b.11 Section 1306.a.11 was not removed. The two sections noted talk about different things. 1308 is about disaster recovery and business continuity planning. The backups created as per section 1306, among other things, are used as part of the recovery processes defined in 1308.
			1306.d.02 The drafting team agrees with your comment and will update the standard accordingly.
			1306.d.03.iii The drafting team respectfully disagrees. Logs are the basis for audit trails.
			1306.e Agreed. The drafting team will review compliance levels for consistency with measures.

Name	Company	Comments	Responses
			1306.e.02 The drafting team agrees with your comment and will update the standard accordingly.
			1306.e.02.ii.C The drafting team agrees and will update the standard accordingly.
			1306.e.03.vii The compliance measures will be reviewed and revised accordingly.

Name	Company	Comments	Responses
Al Cooley	Verano	<p>1303: Page 13, Section 1, 2, iv, Personnel &amp; Training: This section doesn't appear to make provision for the ideal case where preventive measures alert the entity to the fact that it is experiencing a cyber attack. Perhaps it could more effectively read: "Action plans and procedures to react to a detected or potential cyber incident, or to recover or re-establish critical cyber assets and access thereto following a cyber security incident."?</p> <p>1304, Page 17, a, 2, Electronic Access Controls: In order to ensure the perimeter is not breached, authentication should be carried out before the external communication comes in contact with electronic resources within the perimeter. Otherwise it is possible to penetrate the system before authentication takes place. To preclude this scenario, the following could be appended to the last sentence in the first paragraph "...to ensure authenticity of the accessing party, and such authentication shall be carried out before any communication received from the external party is allowed to interact with any asset within the logical perimeter."</p> <p>1304, Page 17, a, 2, Electronic Access Controls: Recognizing the fact that most organizations employ strong technology to manage logical access, many malicious intruders focus their penetration efforts on embedding payloads in legitimate traffic. As a result, technologies at the electronic perimeter are now designed to detect and automatically block such malicious payloads, in addition to managing logical access. The importance of this protection does not appear to come out at present. This section focuses on logical access control, and the section on "Integrity Software" is focused on possible system level tools. While system level integrity tools are both desirable and complementary, in many cases the need for CPU cycles, predictability and/or vendor support may preclude deployment of CPU intensive Integrity Software (e.g. AV, IPS) on the systems themselves. Presumably that is the reason why that section calls for a process governing deployment, rather than directly requiring deployment of the protection software? Consequentially, it would seem desirable to explicitly call out the need for monitoring authorized traffic for malicious payloads at the perimeter, and blocking such payloads. This could be accomplished by adding the following after the second sentence, "They will also ensure that authorized traffic does not contain malicious embedded content."</p> <p>1304, Page 21, f, Sanctions: Despite the efforts of many parties</p>	<p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.06 This observation has been incorporated in the suggested new wording of this requirement for draft 2. Thank you.</p> <p>1306.a.10 This requirement is about "situational awareness" of networked-computing infrastructure. Each responsible entity will have to figure out for itself how it will establish and maintain situational awareness of its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented"</p> <p>1306.e.03 The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
		<p>to address the issue of cyber security in the nation's critical infrastructure, our progress as an industry in making substantive changes has been modest. The standard must provide compliance incentives that are meaningful enough that the security issue receives appropriate attention. 1300 should have mandatory non-compliance penalties that are substantial enough to be meaningful within the context of a specific non-complying entity's financial performance, while not being onerous to other entities. As such penalties should be scaled.</p>	
		<p>1306, Page 26, a, 2, ii, Generic Account Management: Note that today's perimeter technology allows all remote access to be intercepted for authorization purposes on a single user account basis, irrespective of the support provided in the cyber assets for authorization. Since such technology is required to secure the logical perimeter, it can, at no incremental cost, be used to ensure any remote access within the perimeter (systems located in physically unsecured locations within a plant) is granted only to specific authorized individuals. As such, it seems desirable to ensure this technology is implemented if the system does not support individual accounts. For instance, a sentence at the end of this section could be added: "All remote access within the perimeter should utilize the access control technology employed at the perimeter to overcome limitations on individual account access, if any."</p>	
		<p>1306, Page 27, a, 4, Integrity Software: Public reports clearly demonstrate that viruses, worms, Trojans and other malware are one of the most common cyber threats. In section 3, the standard calls for "timely installation of applicable security patches", while in this section the standard only calls for a formally documented process governing the use of preventive measures. It does not appear to call for the timely application of preventive measures, either on the systems themselves and/or at the perimeter, that virtually all corporations today require? Traditionally the focus of electronic security has been preventing outsiders from penetrating the logical perimeter. However statistics show that roughly 50% of successful cyber intrusions are launched from within the perimeter. The vectors for internal incidents vary. Examples include the intentional creation of malware (time bombs, etc.), the alteration of critical system resources by authorized but disgruntled employees, the addition of unauthorized cyber assets to the network by employees/contractors for malicious purposes, etc. There are a variety of different ways to prevent and detect these types of attacks, through procedures that use existing capabilities, or</p>	

Name	Company	Comments	Responses
		<p>through today's automated tools. Given the growing importance of this category of threat, it might be helpful to more explicitly focus on this scenario, and review the language put forth in the rest of the standard from that light. Section 1304 and 1306 would be specific areas of focus. For instance, in this section a slight modification could be made to more explicitly deal with the issue: "System integrity tools must be employed, wherever technically feasible, to prevent, limit exposure to, and/or mitigate creation or importation of email-based, browser-based, file-based and other electronic malware into assets at and within the electronic security perimeter. A formally documented process identifying the deployment strategy, the location and upkeep of such integrity tools shall be maintained and reviewed annually." A similar change is necessary on page 29, section 4: "...a record of all anti-virus, anti-Trojan, file integrity, and other system integrity tools employed ...". A comment on terminology. The wording used in this section may be a little too specific, in a strict sense. The draft calls out Internet-borne threats, while such exploits often enter the perimeter through connections with internal production systems, general corporate networks, removable media, etc. Similarly, viruses are only one intrusion attack vector that current technologies protect against; so broader terminology would be appropriate in various places through the document. For example, the definition on page 31, C) is probably too strict. It might more broadly be worded: "Signature-based integrity software (monthly)", as is the definition of page 31, v: "...are being kept up to date on signature updates..."</p> <p>1306, Page 27, a, 6, Retention of System Logs: Logs are needed for the security tools or processes (if tools are not used) recommended in this draft. It should also be noted that it is possible to use the logs from monitoring tools to provide logging trails for system/applications that do not provide logging. The first sentence might more appropriately read: "All critical cyber security assets and their associated security monitoring systems/procedures must generate an audit trail..."</p> <p>1306, Page 28, a, 10, Operating Status and Monitoring Tools: Since the essence of this standard is ensuring adequate cyber security measures, and since common applications, systems and tools provide security related statistics it would seem quite important to include "security events" in the list of parameters to be monitored. As discussed above, with respect to internal threats, it is very important to monitor and report on key changes at the application level. We suggest the sentence be</p>	

Name	Company	Comments	Responses
		<p>modified as follows: "Communications systems, computers and applications used for operating critical infrastructure must include or be augmented with automated tools to monitor operating state, utilization, performance and security events, at a minimum." A similar change is required on page 30, section 10: "The responsible entity shall maintain documentation identifying organizational, technical and procedural controls, including tools and procedures for monitoring operating state, security events, utilization and performance of critical cyber assets."</p>	
		<p>1306, Page 31, e, 3, x, Levels of Noncompliance: Cyber security issues are extremely hard to detect, because, unlike physical security, it may not be obvious when a severe compromise is underway, or has been completed. As such it seems inappropriate to call out monitoring tools, which will provide the most effective means for detecting a compromise, as N/A. To remedy this, on page 31, Section e, 2, iii a change should be made to read, "Monitoring process and tools are in place, and retention of logs exists (operator, application, intrusion detection, network, perimeter), but a gap of greater than three days but less than seven days exists." Section 3,vii could be similarly modified and section3, x deleted (as it is incorporated above), "Monitoring process and tools are in place, and retention of logs exists (operator, application, intrusion detection, network, perimeter), but a gap of greater than seven days exists." Note the addition of elements called out previously in the draft but previously omitted from this section.</p>	



Name	Company	Comments	Responses
Allen Berman	LIPA	<p>1306 Systems Security Mangement</p> <p>(a)Requirements (2) Account and Password Management (ii) Generic Account Management Comment: "Where technically supported, individual accounts must be used (in contrast to a group account)". Is this necessary in a Control Room that is staffed on a 24x7 basis?</p> <p>(a) Requirements (2) Account and Password Management (iv) Acceptable Use Comment: Suggest changing "... the audit of all account usage to and individually named person.." to "...the audit of all account usage to an individually named person.."</p> <p>Comment: Please clarify what is meant by "personal registration"?</p> <p>(a)Requirements (6) Retention of Systems Logs Comment: Please clarify what is meant by "... security related system events".</p> <p>(a) Requirements (8) Disabling Unused Network Ports/Services Comment: What is meant by term inherent?</p> <p>(a)Requirements (9) Dial-up modems Comment: Is a written policy for following a manual process (i.e. temporarily connecting a normally disconnected modem for maintenance / troubleshooting purposes) an acceptable form of a "secure dial-up modem connection"? If not, what constitutes a secure dial-up connection?</p> <p>(a) Requirements (10) Operating Status Monitoring Tools Comment: Might this be considered more of a performance / reliability issue rather than a security issue?</p> <p>(a) Requirements (11) Back-up and Recovery Comment: The standard states that "Archival information stored on computer media for a prolonged period of time must be tested at least annually to ensure that the information is</p>	<p>1306.a.02 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.02 The drafting team will clarify this sentence. "individually named user accounts and record/update list of all personnel that use group, super-user, and administrator accounts.</p> <p>1306.a.02.ii The intent of the standard is to establish a method for individual accountability.</p> <p>1306.a.06 This is completely situation-dependent, so the responsible entity will have to create valid audit trails for itself by close examination of processes and procedures in operation. 'Events' are distinguished as being more fundamental than 'incidents'; in fact, the latter is often composed of one or more of the former. Examples of events are system administrator execution of privileged commands, both successful and unsuccessful, extended failed login attempts, new account creation, configuration changes, and discovery of network port-probing, to name but a few. At the application level, examples could be logs of system re-directs, or logging of attempts to manually modify production data.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.a.09 Yes</p> <p>1306.a.10 It goes to availability, part of the infosec triad of confidentiality, availability, and integrity. So, yes, it is a reliability measure and part of reliability is availability.</p> <p>1306.a.11 The word 'archival' will be deleted. The intent of the requirement is: 1) back-up what you need to in order to recover from any of a range of contingencies; 2) Move a copy far enough away so the same disaster that got the data center doesn't get the back-ups; 3) test the media periodically to be sure it is still readable should it be necessary to do so.</p> <p>1306.b.01 The drafting team agrees and will update the</p>

Name	Company	Comments	Responses
		recoverable." This appears to be unrelated to Cyber Security. "Archival data" can be interpreted as long-term "historic" data and not backups of critical cyber assets. In this context, what would be the purpose of restoring archival data annually?	standard to state "known" security vulnerabilities.
		(b) Measures (1) Test procedures Comment: How can testing of potential security vulnerabilities be quantified?	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.  1306.b.05 The drafting team respectfully disagrees. Outsourcing does not relieve management of fiduciary oversight responsibility
		(b)Measures (4) Integrity Software Comment: Suggest that the following sentence be reworded for clarity. "Where integrity software is not available for a particular computer platform or other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malware must also be documented."	1306.b.08 Agreed  1306.b.08 Current vendor agreements must be analyzed and modified as appropriate in order to be in compliance with the Standard. Compliance with the Standard would seem to be incumbent upon vendors intending to sell into this market.
		(b) Measures (5) Identification of Vulnerabilities and Responses Comment: This first sentence of this section seems to require that personnel who maintain critical cyber assets have extensive knowledge in technology and techniques for identifying vulnerabilities including the tools and procedures that can identify them. Please clarify this requirement.	1306.b.09 There are numerous approaches that could be taken to fulfill this requirement, each with it own set of (non-exclusive) appropriate actions incumbent to each.  1306.b.10 Refer to Response to comments on section 1306.a.10
		(b) Measures (8) Disabling Unused Network Services/Ports Comment: Re-label this section to read "Disabling Unused Network Ports/Services" to match section (a)(8).	1306.b.11 Refer to Response to comments on section 1306.a.11
		Comment: While some organizations may have the in-house expertise to execute this requirement, others may rely upon vendor support in order to avoid disabling required ports and/or services and impacting their on-line production system. Additionally, a vendor's security solution may be implemented without passing on details to the customer. While unfortunate, the vendor may do this for competitive business reasons. In such a case, accurate configuration documentation would be difficult to maintain.	
		(b)Measures (9) Dial-up Modems Comment: What is meant by "appropriate actions" in the following sentence? "The documentation shall verify that the	

Name	Company	Comments	Responses
		responsible entity has taken the appropriate actions to secure dial-up access to all critical cyber assets."	
		(b) Measures (10) Operating Status Monitoring Tools Refer to comments on section (a)(10).	
		(b) Measures (11) Back-up and Recovery Refer to comments on section (a)(11).	

Name	Company	Comments	Responses
Bill Wagner	Calpine	<p>Page 26, 1306 Systems Security Management, (2) Account and Password Management: Some organizations may implement an authentication system that is stronger than passwords but does not require a password (e.g., Certificate-based or bio-metric authentication). It may be useful to explicitly mention that Account Password Management is only pertinent to accounts that actually use a password for authentication.</p> <p>Page 29, Section 1306 Systems Security Management, (b) Measures, (7) Change Control and Configuration Management, clarify last sentence by striking "all" after "The documentation shall verify that"</p>	<p>1306.a.02 The drafting team agrees this is the intent and will update the standard accordingly.</p> <p>1306.b.07 The drafting team agrees and will update the standard accordingly.</p>

Name	Company	Comments	Responses
Charles Yeung	SPP	<p>1306 (a) (1) Test Procedures: Should "critical cyber security assets" be reworded as "critical cyber assets"? If not, this term needs to be defined.</p> <p>1306 (a) (1) Test Procedures: It is impractical to devise specific procedures to test all known vulnerabilities in an effort to ensure the security patch or alternate mitigation is effective. A reasonable assumption must be made that if all known security patches are installed or alternate mitigation strategies have been implemented, the specific operating system vulnerability has been addressed. Test procedures, in conjunction with the annual controlled penetration test, should confirm that designed security access controls are functioning properly. This could include, for example, verification that multi-factor network access authentication or the requirement for digital certificates to gain access to an application system is not disabled by the update.</p> <p>1306 (a) (2) (iv) Acceptable Use: ". . . usage to and individually named person . . ." should read ". . . usage to an individually named person . . ."</p> <p>1306 (a) (2) (iv) Acceptable Use: What does the term "personal registration" for any generic accounts mean?</p> <p>1306 (a) (3) Security Patch Management: There are occasions where a security patch cannot be applied and no mitigation strategy is available. The standard may want to require the asset owner to work with the vendor to resolve the incompatibility between the system and the patch. Otherwise, the asset owner can just say "hey, cannot fix this" and drop it at that.</p> <p>1306 (a) (10) Operating Status Monitoring Tools: What is the expectation when the automated tools detect a problem? Should the standard prescribe a requirement for notification, or is simply looking at logs and reports some time after the fact good enough? If the latter, then why prescribe the tools at all?</p> <p>1306 (b) (1) Test Procedures: Requirement should be reworded to require documentation of testing of security features or access controls, not vulnerabilities. It is impractical to devise a test procedure for all known vulnerabilities (see comment to 1306 (a) (1) Test Procedures).</p> <p>1306 (b) (2) Account Password Management: The requirement for documentation and verification that accounts comply with</p>	<p>1306.a.01 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.01 The drafting team agrees and will update the standard to reference "known" vulnerabilities.</p> <p>1306.a.02.iv The drafting team will update the standard accordingly.</p> <p>1306.a.02.iv The intent of the standard is that an individual person is associated with the account and manages access to the account by other individuals. The responsible entity should document this individual and all individuals with access to the generic account.</p> <p>1306.a.03 The intent of the standard is to recognize limitations of legacy equipment and the ability to manage the risk with a variety of actions that could avoid upgrades and patches. For example, containing connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.10 This requirement is about "situational awareness" of networked-computing infrastructure. Each responsible entity will have to figure out for itself how it will establish and maintain situational awareness of its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented"</p> <p>1306.b.01 The drafting team agrees testing should include testing for security features and access controls and will add this to the standard. The drafting team disagrees concerning testing of vulnerabilities, the drafting feels testing should include testing for vulnerabilities.</p> <p>1306.b.02 The intent of the standard is that policies are in</p>

Name	Company	Comments	Responses
		<p>the password policy could be construed to require that the password itself be verified. It is hard enough to verify that the password has been changed within a certain period of time on some operating systems. The FAQ, at least, needs to elaborate on this requirement.</p> <p>1306 (b) (3) Security Patch Management: The requirement needs to address layered application patches (e.g. MS Office, Apache, Tomcat, JBoss, Hummingbird Exceed) as well.</p> <p>1306 (b) (4) Integrity Software: Maintaining a record of the version level of the integrity software currently in use is cumbersome and problematic. Most anti-virus products routinely update version levels as part of the scheduled updates, often several times per week. The standard needs to require that the integrity software be maintained up to date and documentation needs to demonstrate how that is done and how it is verified (particularly necessary when the software is configured for automatic, unattended updates).</p> <p>1306 (b) (6) Retention of Logs: This requirement needs to specify the retention period, consistent with retention periods defined elsewhere in the standard.</p>	<p>place to ensure that the password meets the requirement not that passwords themselves be verified. Appropriate evidence should be maintained to support password requirements.</p> <p>1306.b.03 Agreed, the intended interpretation of the standard maintenance of the security profile. The drafting team will address your recommendation in the FAQs.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.06 It's assumed that the comment pertains to clarification as to "calendar days" versus just "days", which could be interpreted to mean "business days."</p>

Name	Company	Comments	Responses
Charlie Salamone	NSTAR	<p>1306.a.2.i - First sentence should read "Where practicable, strong passwords for account must be used in the absence of more sophisticated methods such as multi-factor access controls"</p> <p>1306.a.3 - Remove "and upgrades to" at the end of the 1st sentence.</p> <p>1306.a.3 - Change last sentence to include "business justification must be documented". A compensating measure may not always be an option.</p> <p>1306.a.6 - The standard needs to be more specific on what logs needs to be maintained.</p> <p>1306.e.3.vii - Need to identify what is meant by operator (system administrator or control system operator)</p>	<p>1306.a.02.i Noted. The drafting team feels it is important to use strong passwords at a minimum.</p> <p>1306.a.03 The intent of the standard is to recognize limitations of legacy equipment and the ability to manage the risk with a variety of actions that could avoid upgrades and patches. For example, containing connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.03 The drafting team is in agreement with your comment. It is stated this way because not everyone looks at software updates in the same manner.</p> <p>1306.a.06 This is completely situation-dependent, so the responsible entity will have to create valid audit trails for itself by close examination of processes and procedures in operation. 'Events' are distinguished as being more fundamental than 'incidents'; in fact, the latter is often composed of one or more of the former. Examples of events are system administrator execution of privileged commands, both successful and unsuccessful, extended failed login attempts, new account creation, configuration changes, and discovery of network port-probing, to name but a few. At the application level, examples could be logs of system re-directs, or logging of attempts to manually modify production data.</p> <p>1306.e.03.vii The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
Chris DeGraffenried	NYPA	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p>	Please see response to A. Ralph Rufrano.



Name	Company	Comments	Responses
		<p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1306.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".</p> <p>1306.b.3, remove;</p> <p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p>	

Name	Company	Comments	Responses
		<p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change          "...so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."          to          "...mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;</p> <p>"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence.          Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;          "The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p>	

Name	Company	Comments	Responses
		to "Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."	
		1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"	
		Remove 1306.b.11, since 1306.a.11 was removed.	
		1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."	
		1306.d.3.iii, change "system log files" to "audit trails"	
		1306.e.2, change "the monthly/quarterly reviews" to "the reviews"	
		1306.e.2.ii.C, change "anti-virus" to "malicious"	
		1306, the Compliance levels should be updated to match the above measures.	

Name	Company	Comments	Responses
Dave McCoy	Great Plains Energy	<p>1301, 1303, 1306 -- There are multiple references to the time frame for implementing access changes. (See list of references below.) It would be helpful if the requirements were stated clearly and centralized in one place:</p> <p>1306 (b) Measures (2) Account and Password Management ...that obsolete accounts are promptly disabled. Upon normal movement of personnel out of the organization, management must review access permissions within 5 working days. For involuntary terminations, management must review access permissions within no more than 24 hours.</p>	1306.b.02 The drafting team agrees and will review the standard for consistency.

Name	Company	Comments	Responses
Dave Norton	Entergy Transmission	<p>37. Page 26 - correct the grammar and comma punctuation on 1306 (a) (2) second sentence, "The responsible entity must establish...implemented, and documented that includes...:</p> <p>38. Page 27 - correct grammar typo, (iv) "The policy must support the audit of all account usage to and individually named person."</p> <p>39. Page 28 - last paragraph, 5 lines from the bottom, correct "vender" spelling</p> <p>40. Page 29 - (4) middle of the paragraph, add commas to the string, "...of all</p> <p>41. Page 29 -- "...available updates to these tools security patches/OS upgrades and current revision /patch levels." The last sentence is a fragment that does not make sense, try moving the word "that" from before "are being taken" and placing it instead after malware adding a comma, as in "malware, that must also be documented" or just re-craft the whole sentence.</p> <p>42. Page 29, (5) take out the comma after "vulnerability assessment" in the second sentence.</p> <p>43. Pages 29 (6) and 30 (11): change "index" to "indexes"</p> <p>44. Page 29 - (7) "The documentation shall verify that all the responsible entity follows..." maybe this was meant to say "that all the members of the responsible entity follow a methodical approach to managing changes to their critical cyber assets."?</p> <p>45. Page 29 - (8) and also (9) ...and a record of the regular audit..." What does "regular audit" refer to? Which of the audits discussed are these two in (8) and (9) and how often are they to be performed? Perhaps a reference to another section(s) is needed here.</p> <p>46. Page 30 - (d) (2) "The performance-reset period shall be one year..." What does "performance-reset period" describe?</p> <p>47. Page 30 - (e)(1)(i) Levels of Non-Compliance Level one, take out the word "have" in "...but have does not cover..."</p> <p>48. Page 31 - (e) Levels of Non-Compliance (2) Level two (ii) Rewrite this non-compliance to make its meaning and intent clearer to the reader. It reads "Test Procedures: Document(s)</p>	<p>1306.a.02 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.02.iv The drafting team will update the standard accordingly.</p> <p>1306.b.03 The comment is noted.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.05 updated</p> <p>1306.b.06 OK</p> <p>1306.b.07 The drafting team agrees and will update the standard accordingly.</p> <p>1306.b.08 The word "annual" will replace the word "regular"</p> <p>1306.d.02</p> <p>1306.e.01.i The drafting team agrees and will update the standard accordingly.</p> <p>1306.e.02.ii The drafting team agrees with your comment and will update the standard accordingly.</p> <p>1306.e.03.iii.A The compliance measures will be reviewed and revised accordingly.</p> <p>1306.e.03.ix The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
		<p>exist, but documentation verifying that changes to critical cyber assets were not tested in scope with the change."</p>	
		<p>49. Page 31 - (e) Levels of Non-Compliance (3) Level three:            (iii) A) "Document(s) exist but documentation verifying (____) accounts and passwords comply with the policy does not exist and/or" This would be less awkward if we put the word "that" between the words "verifying" and "accounts."</p>	
		<p>50. Page 31 - (3) (ix) and (x) if these two items are "N/A," remove them from the non-compliance criteria listings.</p>	

Name	Company	Comments	Responses
David Kiguel	Hydro One	<p>In 1306.b.3 Change</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability.</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>In 1306.b.6, change</p> <p>"The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p> <p>to</p> <p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis."</p> <p>In 1306.a.1, last paragraph, modify the second sentence - Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible.</p> <p>Change "pooding" and "puffing" to "putting" in 1306.a.2.ii</p> <p>Remove "Generic" from the title of 1306.a.2.ii</p> <p>In 1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>In 1306.a.3 change</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets.</p>	<p>1306.a.01 The drafting team feels a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.</p> <p>1306.a.02.ii The drafting team will update the standard accordingly.</p> <p>1306.a.02.ii The intent of this sub-section is to address group type accounts and not individual accounts.</p> <p>1306.a.02.iii The drafting team feels reviews should be conducted more frequently than annually.</p> <p>1306.a.03 The drafting team is in agreement with your comment. It is stated this way because not everyone looks at software updates in the same manner.</p> <p>The intent of the standard is to recognize limitations of legacy equipment and the ability to manage the risk with a variety of actions that could avoid upgrades and patches. For example, containing connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.06 This is completely situation-dependent, so the responsible entity will have to create valid audit trails for itself by close examination of processes and procedures in operation. 'Events' are distinguished as being more fundamental than 'incidents'; in fact, the latter is often composed of one or more of the former. Examples of events are system administrator execution of privileged commands, both successful and unsuccessful, extended failed login attempts, new account creation, configuration changes, and discovery of network port-probing, to name but a few. At the application level, examples could be logs of system re-directs, or logging of attempts to manually modify production data.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create</p>

Name	Company	Comments	Responses
		<p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets. Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>In 1306.a.4 Change</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>In 1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>In 1306.a.6 change</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three years in an exportable format, for possible use in further event analysis."</p> <p>In 1306.a.7 Remove "Configuration Management" from the Title</p> <p>In 1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>Request clarification of 1306.a.10. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p>	<p>an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>1306.a.07 The drafting team acknowledges your comments and this topic will be addressed as a governance item covered in section 1301.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.a.10 Inadequate "situational awareness" was a finding from the investigation of the NE blackout of 2003, and this requirement is about situational awareness of networked-computing infrastructure deemed to be critical cyber assets, particularly host computers and high-speed data communications lines. Salient things to monitor can include CPU utilization, memory utilization, running processes, disk partition usage, hung daemons, defunct process queues, line/network throughput, denial of service attacks, and so on...</p> <p>Each responsible entity will define, implement, and document what it needs to monitor in order to establish and maintain situational awareness of its set of critical cyber assets in operation. The permuted combinations of automated and process tools that might be employed are many and situation-dependent.</p> <p>The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented"</p>



Name	Company	Comments	Responses
		Remove 1306.a.11 since 1308 addresses back-up and recovery.	1306.a.11 The two sections noted talk about different things. 1308 is about disaster recovery and business continuity planning. The backups created as per section 1306, among other things, are used as part of the recovery processes defined in 1308.
		In 1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.	
		In 1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".	1306.b.01 The drafting team will update the standard such that a requirement exists for documenting the test environment, but not necessarily in the procedures. The update will also replace potential with known.
		In 1306.b.3, remove "The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."	The drafting team feels a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.
		In 1306 b.3 first sentence-eliminate the word "management".	1306.b.02 The drafting team agrees and will update the standard accordingly.
		In 1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.	1306.b.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.
		1306.b.4 third sentence Change "so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware." to "mitigate risk of malicious software".	1306.b.03 The comment is noted.  1306.b.03 Agreed, because the word "approved" implies authorization and oversight.
		1306.b.4 Remove the second sentence.	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.
		1306.b.4 Replace the fourth sentence with "Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.  1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.
		In 1306.b.5, remove the first sentence. Based on a third party outsourcing of this associated work of vulnerability assessment.	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.
		1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"	1306.b.05 The drafting team respectfully disagrees. Outsourcing does not relieve management of fiduciary oversight responsibility
		Remove 1306.b.11, since 1306.a.11 was removed.	
		In 1306.d.2, change "The compliance monitor shall keep audit records for three years."	1306.b.06 The drafting team respectfully disagrees. Logs are the basis for audit trails, and logs record "events." An audit trail can and usually is at least in part comprised of event log data. So, it is event logs that must be retained, to support the

Name	Company	Comments	Responses
		to "The compliance monitor shall keep audit records for three calendar years."	audit trail. An audit trail can be thought of as (documentation of) a "control process," part of which consists of event logs.
		In 1306.d.3.iii, change "system log files" to "audit trails"	1306.b.07 The drafting team agrees and will update the standard accordingly.
		In 1306.e.2, change "the monthly/quarterly reviews" to "the reviews"	1306.b.11 Section 1306.a.11 was not removed. The two sections noted talk about different things. 1308 is about disaster recovery and business continuity planning. The backups created as per section 1306, among other things, are used as part of the recovery processes defined in 1308.
		In 1306.e.2.ii.C, change "anti-virus" to "malicious"	
		In 1306, the Compliance levels should be updated to match the above measures.	1306.d.02 The drafting team agrees with your comment and will update the standard accordingly.
			1306.d.03.iii The drafting team respectfully disagrees. Logs are the basis for audit trails.
			1306.e Agreed. The drafting team will review compliance levels for consistency with measures.
			1306.e.02 The drafting team agrees with your comment and will update the standard accordingly.
			1306.e.02.ii.C The drafting team agrees and will update the standard accordingly.

Name	Company	Comments	Responses
David Little	Nova Scotia Power	<p>1306</p> <p>In 1306.a.1, last paragraph, modify the second sentence to read as follows; Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible.</p> <p>1306.a.2.ii remove Generic from the title</p> <p>1306.a.2.iii, use at least annually instead of at least semi-annually</p> <p>Change 1306.a.3 from; A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets to A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets. ." (upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented.</p> <p>Change 1306.a.4 from; A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter. to A formally documented process governing mitigation of the importation of malicious software into critical cyber assets.</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>Change 1306.a.6 from All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis.</p> <p>to</p> <p>It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three years in an exportable format, for possible use in further event analysis.</p> <p>1306.a.7 Remove Configuration Management from the Title</p> <p>1306.a.8 Remove the word inherent it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove Test procedures must also include full detail of the environment used on which the test was performed. Also replace potential with known in the last sentence. Also in the last sentence insert the words if possible at the end of the sentence.</p> <p>1306.b.2, instead of 24 hours use the above wording on 24 hours for cause, or seven days.</p> <p>1306.b.3, remove;</p> <p>The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels.</p> <p>and change</p> <p>The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability.</p> <p>to</p> <p>The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to</p>	

Name	Company	Comments	Responses
		<p>minimize the risk of a critical cyber asset compromise from a known security vulnerability.</p> <p>In 1306 b.3 first sentence-eliminate the word management</p> <p>1306.b.4, remove anti-virus, anti-Trojan, and other from the first sentence.</p> <p>1306.b.4 third sentence Change ..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware. to ..mitigate risk of malicious software.</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with; Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented.</p> <p>1306.b.5 remove the first sentence. Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from; The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets. to Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis.</p> <p>1306.b.7 In the final sentence remove the word all and change the heading by deleting and Configuration Management</p> <p>Remove 1306.b.11, since 1306.a.11 was removed.</p> <p>1306.d.2, change from The compliance monitor shall keep audit records for three years. to The compliance monitor shall</p>	

Name	Company	Comments	Responses
		keep audit records for three calendar years	
		1306.d.3.iii, change system log files to audit trails	
		1306.e.2, change the monthly/quarterly reviews to the reviews	
		1306.e.2.ii.C, change anti-virus to malicious	
		1306, the Compliance levels should be updated to match the above measures.	

Name	Company	Comments	Responses
Deborah Linke	US Bureau of Reclamation	<p>1306</p> <p>(1) Test Procedures: All new systems and significant changes to existing critical cyber security assets must use documented information security test procedures to augment functional test and acceptance procedures. Significant changes include security patch installations, cumulative service packs, release upgrades or versions to operating systems, application, database or other third party software, and firmware. - This should also include changes (not patches) that may be made by the responsible entity, the entity's contractors, or the product vendors. Patches are assumed to be those modifications made to S/W, F/W to address coding errors. Changes are those modifications made to address new or different functionality requirements. Both change and patch management processes should be a part of the security controls required on critical cyber assets covered under this standard. Testing is required under both scenarios, but the testing is different in each case.</p> <p>(iv) Acceptable Use The responsible entity must have a policy implemented to manage the scope and acceptable use of the administrator and other generic account privileges. The policy must support the audit of all account usage to and individually named person, i.e., individually named user accounts, or, personal registration for any generic accounts in order to establish accountability of usage. - The acceptable use policy should address all users, not just those who have administrator or generic access accounts. It should address types of activities allowed (e.g., controlling a power system in accordance with appropriate SOPs through Operator accounts) and types of activities disallowed (e.g., loading unauthorized applications or games, or surfing inappropriate sites -- where web access is permitted).</p> <p>(8) Disabling Unused Network Ports/Services The responsible entity shall disable inherent (unnecessary default) and unused services.</p> <p>(9) Dial-up modems</p>	

Name	Company	Comments	Responses
		<p>The responsible entity shall secure dial-up modem connections. - Security mechanisms could include dial-back technologies, disconnection except when specifically required, and monitoring of activity when the modem is in service.</p> <p>(10) Operating Status Monitoring Tools</p> <p>Computer and communications systems used for operating critical infrastructure must include or be augmented with automated tools to monitor operating state, utilization, and performance, at a minimum. - It is assumed that the function of such tools is to look for and alarm on "abnormal" conditions after tools have had an adequate time to "learn" normal operating conditions. This is not clear as written.</p> <p>(11) Back-up and Recovery</p> <p>Information resident on computer systems used to manage critical electric infrastructure must be backed-up on a regular basis and the back-up moved to a remote facility. Archival information stored on computer media for a prolonged period of time must be tested at least annually to ensure that the information is recoverable. - It may be necessary to define what constitutes a remote facility (one located more than one mile from the primary facility and in a direction that is likely to be accessible under adverse conditions -- such as floods) Also consider indicating physical and access protection requirements to the storage location to be as stringent as those required for the primary site. Finally, there does not appear to be any requirement listed for marking/identifying backup media.</p>	



Name	Company	Comments	Responses
Dennis Kalma	AESO	<p>1306.a.2 Compliance in legacy systems may not be possible and replacement systems may be the only solution.</p> <p>1306.b.2 It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions.</p> <p>1306.b.11 Should contain specific retention periods.</p>	

Name	Company	Comments	Responses
Doug Van Slyke	ATCO Electric	<p>Section 1301.a.6 - Authorization to Place Into Production</p> <p>This section requires more clarification. Would the SCADA/EMS vendor qualify as an approving authority for changes that are made to customized programs? If not, who would? If the SCADA/EMS vendor sends us a patch and we test it and it appears acceptable from the testing we have done can we approve it. I can see there would be reluctance from our IT group to stamp a patch as APPROVED without being able to review the code changes which is not practical or even allowed with most vendors. On the security side, would we need to have a security expert approve our configuration changes any time we made a change to the firewall or security settings? None of our IT group members are certified security experts.</p>	

Name	Company	Comments	Responses
Ed Goff	Progress Energy	<p>1306 Systems Security Management</p> <p>We assume this include the network gear that makes the perimeter? If so, that needs to be made clear.</p> <ul style="list-style-type: none"> <li>- a.1 - Test Procedure [page 26] - and firmware. - What is meant by 'firmware' here? Does it refer to hardware firmware, bios firmware, ...? Just not quite clear. It may be a good idea to include more specifics and / or examples.</li> <li>- a.2 - Requirement to audit user activity - To what level must user activity be monitored and audited? Enabling auditing at a detail level to track every user action such as what files were opened, and what records changed within the file has the potential to impact system performance, especially for existing systems in operation. Depending on the level of detail required, existing systems in current operations may not have the capability to meet such a requirement.</li> <li>- a.3 -- timely installation -- it is not clear how quickly patches need to be installed.</li> <li>- a.9 -- Secure dial-up -- list criteria of secure dial-up</li> <li>- b.3 Security Patch Management - Including a monthly review record of all available vendor security patches should not be part of inventory. Not all available vendor security patches are applicable to individual company configurations.</li> <li>- a.2.7 -- numbering seems to be off in all of section 2.</li> <li>- a.2.7 -- Change Control and Configuration Management -- this seems to include configuration parameters on PLCs and Alarm Set Points. Is this realistic?</li> </ul>	

Name	Company	Comments	Responses
Ed Riley	CAISO	<p>1306.a.1 Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment. The last sentence is an adequate statement.</p> <p>1306.a.2.i Should qualify "strong password" as to where it is technically supported. Not all technology allows for this.</p> <p>1306.a.2.iii Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>1306.a.3 The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.</p> <p>1306.a.4 Needs to state that it will exist "where applicable as defined by the entity".</p> <p>1306.a.6The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible".</p> <p>What is the definition of "security related system events"?</p> <p>1306.a.7 This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency.</p> <p>What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?</p> <p>1306.a.11 This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.</p> <p>1306.b.11 The responsible entity must identify in its policy a minimum retention period satisfactory to reconstruct a critical cyber asset.</p> <p>1306.e.3.vii These specific logs have not been referred to previously in this section of the standard, yet the standard is requiring compliance.</p>	

Name	Company	Comments	Responses
Ed Stein	FirstEnergy	<p>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</p> <p>1306 -- System Security management</p> <p>While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.</p> <p>Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.</p> <p>ABC requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.</p> <p>ABC is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit.</p> <p>Recommendation: Either significantly lessen requirements or eliminate many of the following.</p> <p>-- Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information loses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.</p> <p>-- Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work,</p>	<p>1306.a.01 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections.</p> <p>1306.a.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections.</p> <p>1306.a.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections.</p> <p>1306.a.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections.</p> <p>1306.a.02 The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The drafting team feels employees terminated for cause pose a possible threat and should have access rights removed with 24 hours. Routine are given 7 calendar days to allow for normal business processing to remove rights.</p> <p>1306.a.02 The drafting team agrees with your comment and</p>

Name	Company	Comments	Responses
		<p>but what is the point?</p> <p>-- Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not reasonable.</p> <p>-- Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.</p> <p>-- Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.</p> <p>-- Page 27: Testing "...provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.</p> <p>-- Page: 27 Test Procedure Measures: Language states, "...Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production..." It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.</p> <p>-- Page 29: Integrity software: ABC is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.</p> <p>-- Page 27: Security Patch Management: ABC seeks</p>	<p>will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. . The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p>

Name	Company	Comments	Responses
		<p>clarification of "...upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.</p> <p>-- Page 27: Created formalized change control &amp; configuration management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.</p> <p>Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,</p> <p>-- Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.</p> <p>-- Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.</p> <p>ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?</p> <p>Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, ...no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1301) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <p>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</p> <p>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</p> <p>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</p> <p>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</p>	

Name	Company	Comments	Responses
		<p>ABC recommends:</p> <ul style="list-style-type: none"> <li>- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence.'</li> <li>- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.</li> </ul>	
		<p>Further on the subject of Access requirements, commentors stated that the 24-hour access limitation for updating records was un-duly severe in the Standard 1200 comments. NERC Responses to Cyber Security Standard 1200 Ballot Comments 6-11-03 posted to the NERC website provided the following:</p>	
		<p>"NERC acknowledges the validity of these comments and will address them more fully in the final standard... we will expect that a system will be in place to periodically update access authorization lists on at least a quarterly basis. That protocol will also ensure that access be suspended as soon as possible and no later than 24 hours for those persons who have exhibited behavior, as determined by the organization, suggesting that they pose a threat to the reliability of critical systems. Routine administrative changes resulting from retirements, resignations, leaves, etc. should be handled within the normal course of business but not in excess of three business days after occurrence...."</p>	
		<p>While ABC acknowledges that Standard 1300 is a different standard from 1200, we wish to remind NERC of the statement that they will address objections to the excessively stringent 24 hour access update requirement in the 'final standard.'" Since objections have not been addressed, NERC still needs to do this.</p>	
		<p>Regarding requirements for updating access records, ABC recommends:</p> <p>(1) The requirement should be stated as recommended by NERC above 'Access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that</p>	



Name	Company	Comments	Responses
		<p>they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <p>(2) The requirement should only be defined in one section of the document rather than currently proposed language which includes multiple conflicting requirements within the same Standard.</p> <p>(3) If the item is used to identify non-compliance, all references throughout the document should reflect the revised requirements.</p>	

Name	Company	Comments	Responses
Ernst Everett	OGE	<p>Section 1306 - The requirements in this area are excessive. There should be different requirements for the master station equipment and equipment at remote locations. Even on the master, the documentation and logging requirements are excessive. It should recognize not all legacy equipment will have the capabilities described. Note these are desired goals to work toward, with it being a requirement if the equipment has the capability.</p> <p>Section 1306 - Security Patch Management It may not always be practical to take a compensating measure. The situation should be assessed and documented as to steps taken and why or why not.</p> <p>Section 1306 - Identification of Vulnerabilities Penetration testing is probably not required or worth the cost. Perhaps a requirement for an annual internal assessment with an outside vendor assessment every three years might be more appropriate.</p>	<p>1306.a.01 The drafting team will revise the standard to distinguish requirements between manned and unmanned facilities.</p> <p>The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.03 The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or network isolation.</p> <p>1306.a.05 The intent of the standard is not to have an external vendor perform an assessment. The intent is testing is performed annually for detecting vulnerabilities.</p>

Name	Company	Comments	Responses
Francis Flynn	National Grid	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.i Change from: In the absence of more sophisticated methods, e.g., multi-factor access controls, accounts must have a strong password.</p> <p>to:</p> <p>At a minimum, accounts must have a strong password.</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (some saw these words when the Adobe document was converted into a Word document.)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.ii Change from: Where individual accounts are not supported, the responsible entity must have a policy for managing the appropriate use of group accounts that limits access to only those with authorization...</p> <p>to:</p> <p>The responsible entity must have a procedure for managing the appropriate use of accounts that limits access to only those with authorization...</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets."</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>Change 1306.a.6 from: Retention of Systems Logs</p> <p>to:</p> <p>Systems Logs</p> <p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for one years in an exportable format, for possible use in further event analysis."</p> <p>Add to 1306.a.6 All system logs generated within a security perimeter will be synchronized to a common time source.</p> <p>1306.a.7 Remove "Configuration Management" from the Title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What is being monitored? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p>	

Name	Company	Comments	Responses
		<p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days" as mentioned in earlier comments.</p> <p>1306.b.3, remove;</p> <p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>In 1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence and add the following to the end of the : , excluding the version of the signature files used by these tools.</p> <p>1306.b.4 third sentence Change  ".so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."</p> <p>to</p>	

Name	Company	Comments	Responses
		<p>"..mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;</p> <p>"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence. Based on a third party outsourcing of this associated work of vulnerability assessment.</p> <p>Change 1306.b.6 from;</p> <p>"The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p> <p>to</p> <p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three years in an exportable format, for possible use in further event analysis."</p> <p>1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"</p> <p>1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."</p> <p>1306.d.3.iii, change "system log files" to "audit trails"</p> <p>1306.e.2, change "the monthly/quarterly reviews" to "the reviews"</p> <p>1306.e.2.ii.C, change "anti-virus" to "malicious"</p> <p>1306.e.3.vii</p> <p>The description of non-compliance includes details not included</p>	

Name	Company	Comments	Responses
		in the requirements or measures regarding logs. The statements should be consistent.	
		1306, the Compliance levels should be updated to match the above measures.	

Name	Company	Comments	Responses
Gary Campbell		<p>1306</p> <p>General : Where the word "must" has been used, rewrite to incorporate "shall and should" as appropriate. This is keeping with the NERC direction for standards, I believe.</p> <p>the "requirements" section set the minimum at least or define what is acceptable, the "measures" section tell me what to go and look for and "levels of compliance" section tell me the degree of severity for not having the requirements met. The authors of these requirements in some cases intertwined these three areas, especially the requirements and measures sections. In some areas of the requirements section, it is used as an introductory section explaining what is meant by a specific term presented.</p> <p>Levels of Compliance</p> <p>(i) What documents are to exist, the CM should not be deciding what encompasses this statement, nor should the CM be trying to determine the specific items. We need to be more definitive and less vague</p> <p>3 (iii) What does this mean? Some CM may not in depth knowledge of cyber security or it some the specifics must be clearly defined.</p> <p>3(iv) What constitutes incomplete. If one item of those mentioned can not be found is the entity incomplete?</p> <p>3(v) How can a document verify that all critical cyber assets are being kept up to date?</p> <p>3(ix &amp; x) What does N/A mean? Not applicable or not available? We need to be more explicit.</p> <p>4 No document exists. What documents? None of the documents or one of the documents, exactly which documents if they do not exist will be level 4. Do alternate plans qualify for existing documentation?</p>	<p>1306 The drafting team agrees with your comment and will revise the draft accordingly.</p> <p>1306.a.01 The drafting team agrees with your comment and will revise the draft accordingly.</p> <p>1306.e.03 The compliance measures will be reviewed and revised accordingly.</p>



Name	Company	Comments	Responses
Guy Zito	NPCC	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24</p>	

Name	Company	Comments	Responses
		hours for cause, or seven days".	
		1306.b.3, remove;	
		"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vendor security patches/OS upgrades and current revision/patch levels."	
		and change	
		"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."	
		to	
		"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."	
		1306 b.3 first sentence-eliminate the word "management".	
		1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.	
		1306.b.4 third sentence Change	
		"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."	
		to	
		"..mitigate risk of malicious software".	
		1306.b.4 Remove the second sentence.	
		1306.b.4 Replace the fourth sentence with;	
		"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."	

Name	Company	Comments	Responses
		<p>1306.b.5 remove the first sentence.</p> <p>Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;</p> <p>"The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p> <p>to</p> <p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"</p> <p>Remove 1306.b.11, since 1306.a.11 was removed.</p> <p>1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."</p> <p>1306.d.3.iii, change "system log files" to "audit trails"</p> <p>1306.e.2, change "the monthly/quarterly reviews" to "the reviews"</p> <p>1306.e.2.ii.C, change "anti-virus" to "malicious"</p> <p>1306, the Compliance levels should be updated to match the above measures.</p>	

Name	Company	Comments	Responses
Hein Gerber	British Columbia Transmission Corp.	1306 -- Systems Security Management Paragraph (b)(2) requires management to review access permissions for involuntary terminations within 24 hours. This review period is too long. Responsible entities should revoke access permissions for involuntary terminations PRIOR to the employee being informed of their termination.	1306.b.02 The drafting team agrees the permissions should be changed as soon as possible. The 24 hour time period is to allow for changes when termination is not known in advance and to provide a measure for verification.

Name	Company	Comments	Responses
Howard Ruff	WE Energies	<p>Section 1306, Systems Security Management, item 5, Identification of vulnerabilities and responses. Can the annual vulnerability assessment be performed by internal staff? Will only an external, impartial auditor be accepted? Also, this section may not be applicable for power plant and substation control systems due to their proprietary nature and age. A different systems security management section may be warranted to address these instances.</p>	<p>1306.a.05 The intent of the standard is not to have an external vendor perform an assessment. The intent is testing is performed annually for detecting vulnerabilities either by internal staff or external auditors.</p> <p>The standard will be revised to distinguish between manned and unmanned facilities (i.e. substations)</p>

Name	Company	Comments	Responses
Jim Hiebert	WECC EMS WG	<p>1306.a.1 Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment. The last sentence is an adequate statement.</p> <p>1306.a.2.i Should qualify "strong password" as to where it is technically supported. Not all technology allows for this.</p> <p>1306.a.2.iii Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>1306.a.3 The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches.</p> <p>1306.a.4 Needs to state that it will exist "where applicable as defined by the entity".</p> <p>1306.a.6 The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible".</p> <p>What is the definition of "security related system events"?</p> <p>1306.a.7 This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency.</p> <p>What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?</p> <p>1306.a.11 This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.</p>	<p>1306.a.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.</p> <p>1306.a.02.i The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02.iii The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections.</p> <p>1306.a.03 The drafting team agrees with your comment and will revise the draft accordingly.</p> <p>The intent of the standard is to recognize limitations of legacy equipment and the ability to manage the risk with a variety of actions that could avoid upgrades and patches. For example, containing connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team believes a formally documented process governing mitigation of the importation of malicious software into critical cyber assets of some form is applicable to each entity.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p>

Name	Company	Comments	Responses
			<p>1306.a.07 A review of the standard will be conducted for consistency between sections.</p> <p>The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The intent is to provide as much separation as possible from production systems. The entity should determine the appropriate level of separation for their environment.</p> <p>1306.a.11 The intent is not to address archival data but to ensure that backup media is tested to ensure data is recoverable. Just the word “archival” shall be stricken.</p>



Name	Company	Comments	Responses
Joanne Borrell	First Energy Services	<p>1306 -- System Security management</p> <p>While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.</p> <p>Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.</p> <p>ABC requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.</p> <p>ABC is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.</p> <p>-- Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information loses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.</p> <p>-- Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?</p> <p>-- Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not</p>	<p>1306 The drafting team believes the standards as presented provide a minimum best practices approach to ensuring cyber security.</p> <p>1306.a.01 The intent of the standard is not that every minor change be documented and tested. The standard states, new systems and SIGNIFICANT changes be tested and documented.</p> <p>1306.a.01 The standard will be updated to "known" vulnerabilities instead of "potential".</p> <p>1306.a.01 The intent of the standard is not that every change be documented and tested. The standard states, new systems and SIGNIFICANT changes be tested and documented in a controlled non-production environment.</p> <p>1306.a.02.iii The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02.iii The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes.</p> <p>1306.a.03 Significant changes include major product releases. Major releases are significant enough to potentially affect security controls and should be tested.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the</p>

Name	Company	Comments	Responses
		reasonable.	critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."
		-- Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.	
		-- Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.	1306.a.07 Testing is a subset of Configuration Management. Configuration Management will be moved to section 1301 Governance.
		-- Page 27: Testing "...provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.	1306.a.10 Inadequate "situational awareness" was a finding from the investigation of the NE blackout of 2003, and this requirement is about situational awareness of networked-computing infrastructure deemed to be critical cyber assets, particularly host computers and high-speed data communications lines. Salient things to monitor can include CPU utilization, memory utilization, running processes, disk partition usage, hung daemons, defunct process queues, line/network throughput, denial of service attacks, and so on.
		-- Page: 27 Test Procedure Measures: Language states, "...Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production..." It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.	Each responsible entity will define, implement, and document what it needs to monitor in order to establish and maintain situational awareness of its set of critical cyber assets in operation. The permuted combinations of automated and process tools that might be employed are many and situation-dependent.
		-- Page 29: Integrity software: ABC is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.	The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented"
		-- Page 27: Security Patch Management: ABC seeks clarification of "...upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.	1306.a.10 That was not the intent. Monitoring is required only for critical cyber assets, as they are defined.
		-- Page 27: Created formalized change control & configuration	1306.a.11 The intent of the standard is not to dictate a retention policy. The information and data to be backed-up should be sufficient to restore the system to production state following a cyber security incident. The retention cycle to support this should be determined by the entity's environment

Name	Company	Comments	Responses
		<p>management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.</p> <p>Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,</p> <ul style="list-style-type: none"> <li>-- Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.</li> <li>-- Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.</li> </ul> <p>ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?</p> <p>Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, ...no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1301) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>ABC recommends:</p> <ul style="list-style-type: none"> <li>- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose</li> </ul>	<p>and risk assessment.</p> <p>1306.b.02 The drafting team agrees and will review the standard for consistency.</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.04 The standard will be updated to more properly match intent, that a process for governing mitigating of the importation of malicious software into critical cyber assets. It is possible this could be accomplished by isolation.</p>

Name	Company	Comments	Responses
		<p>a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <ul style="list-style-type: none"> <li>- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.</li> </ul>	

Name	Company	Comments	Responses
John Blazeovitch	Exelon	<p>1306.a.2.iii This access review requirement appears to be redundant with 1301.a.5.iii and 1303.l.4.iii. We recommend that the access control requirements should only appear in one section of the standard.</p> <p>1306.b.2 We recommend that the access permission review occur within 24 hours for not only involuntary terminations, but also for suspensions.</p> <p>1306.a.6 This section begins: All critical cyber security assets... We recommend that the sentence read: All critical cyber assets...</p> <p>This section requires that the critical cyber asset must generate an audit trail for ALL security related system events. Audit capabilities will vary by system. Enabling full security audit functionality can generate a tremendous volume of events that have minimal or no value, can significantly impact system performance, and can greatly increase storage capacity requirements. We recommend that the responsible entity define requirements for security events that must be generated and to implement system auditing based on those requirements to the extent supported by the system.</p> <p>1306.a.8 The use of the term inherent services is not clear. We recommend that the sentence read: The responsible entity shall disable unused services.</p> <p>1306.b.2 The access review measurement is not consistent with 1301.a.5.iv. The measurement in 1306 is clearer and more complete than the one in 1301.</p> <p>1306.b.10 and 1306.b.11 We recommend that these sections read: ...shall maintain documentation...</p> <p>1306.e.3.iii.B Unmatched reference to 5.3.3.2</p>	<p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>1 306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.10 Yes, thank you. 1 306.b.11 Noted. Thank you.</p> <p>1306.e.03.iii.B The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
John Hobbick	Consumers Energy	<p>1306 -- Systems Security Management</p> <p>3) requires that if the "installation of the patch is not possible, a compensating measure(s) must be taken and documented." This sentence is not consistent with the previous one, which recognizes reasons for not installing patches. It should be revised as follows, "installation of the patch is not possible, but necessary, a compensating measure(s) must be taken and documented." It is quite possible that not only might a patch not be installable, but it could be completely unnecessary, as the problem it is intended to fix, is not applicable to the configuration the software or hardware is connected in. In this case, compensating measure(s) are not necessary.</p> <p>4) Integrity Software Where available -- there are platform availability issues</p> <p>6) Retention of System Logs Exportable format is not always possible, some of the legacy systems only have paper</p> <p>10) Operating Status Monitoring Tools Implementation plan for this item is new functionality and will need 3 years to implement. This is new requirement and time is needed to gather/implement the tools to accomplish. This requirement should only apply to Control Room / EMS type applications, not substation and plant systems.</p> <p>11) Back-up and recovery What does storage of archival information have to do with security?</p>	<p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>1306.a.04 Where integrity software is not available for a particular computer platform then other compensating measures should be taken to minimize the risk of a critical cyber asset compromise from malicious software and must also be documented.</p> <p>1306.a.06 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.10 A valid comment and consideration. While the Implementation Plan for 1300 is still being conceived, the intent is to have this requirement in force for data centers near term, with a more gradual phase-in of requirements for cyber assets operating outside of data center premises.</p> <p>1306.a.11 Generally Accepted Systems Security Principles (GASSP) defines the scope of information security, or 'cyber security', as "anything affecting confidentiality, availability, and integrity of information. That's the gospel. Back-up and recovery is a main component for maintaining both availability and integrity of information... The word 'archive' will be deleted.</p>

Name	Company	Comments	Responses
John Lim	Con Ed	<p>In 1306,</p> <p>Account and Password Management: In some legacy systems, there may not be any account or password management capabilities. The requirement should provide the capability for the entity to claim a waiver for this section in such cases.</p> <p>Vulnerability Assessment: a vulnerability assessment of the critical bulk electric cyber assets may be part of the overall organization's full vulnerability assessment program. These assignments can take up to 3 months to complete in a large organization. We suggest that the requirement be changed from "annual" to "at least once every 2 years".</p>	<p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.03 The drafting team will take this under consideration.</p> <p>Newer network equipment has much of this capability built in.</p> <p>Risks to older networks and equipment can be mitigated by air gap isolation from the Internet or corporate network.</p>

Name	Company	Comments	Responses
Karl Tammer	ISO-RTO Council	<p>1306.a.3 The word ‘timely’ does not adequately reflect the risk management approach that should be used in applying patches.</p> <p>1306.b.2 It is not reasonable to expect a manager to sit at a terminal or otherwise review all access permissions. Management must "ensure" the review.</p> <p>1306.b.11 The company must identify in its policy a minimum retention period satisfactory to reconstruct a critical cyber asset.</p> <p>1306.e.2 (i) and (ii): More clarity is required around these specific reviews.</p> <p>1306.e.3 (vii): These specific logs have not been referred to previously in this section of the standard yet we are being graded on these in compliance.</p>	<p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly.</p> <p>1306.b.11 So noted.</p> <p>1306.e.02 The intent of the standard is that documentation will be checked to ensure that it is up to date with the entity’s environment.</p> <p>1306.e.03 The compliance measures will be reviewed and revised accordingly.</p>



Name	Company	Comments	Responses
Ken Goldsmith	Alliant Energy	<p>1306 Systems Security Management</p> <p>This section has good security principles and appears to have been written for control centers and energy management systems. The same principles may not be applied to all critical cyber assets in generation and transmission. Proprietary software and vendor maintained software require a different set of controls. Test systems may not be an option, mal-ware may not be supported on each system, audit trails not available. Because of the various types of systems, the levels of compliance are not feasible.</p> <p>Suggest a reference to ensure non-critical cyber assets within the same electronic perimeter have appropriate controls to protect the critical asset.</p> <p>Article a-3 Security patch management is a risk based decision and not all critical cyber assets have the same level of risk. If a patch is not installed, it should be documented and a compensating measure may not be required.</p> <p>Article a-5 Remove "(controlled penetration testing)" as this could cause more risk to the asset.</p> <p>Article b-2 Account and Password Management should be removed from this section as it is already addressed in 1301.</p>	<p>1306The standard will be enhanced to differentiate between attended and unattended locations.</p> <p>1306 Non-critical cyber assets within the perimeter must be secured to the extent they present a risk to the critical cyber assets.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>1306.a.05 Reference to penetration test removed.</p> <p>1306.b.02 The intent of this section is to address mechanics of account and password management on the systems.</p>

Name	Company	Comments	Responses
Larry Brown	EEl Security Committee	<p>Section 1306</p> <p>FIRST -- Overall, this standard is far too detailed and onerous for all cyber equipment, especially for non-critical cyber facilities that happen to be located within a secured critical cybersecurity perimeter (or as otherwise determined through the corporate cybersecurity risk assessment to be of little concern). For such equipment, there are much simpler means to assure security, such as securing the communications path -- see comment above at Section 1302(a)(2)(i)(D). Examples of such equipment include that using dial-up access at substations or transmission and generation facilities. For instance, given the number of pieces of non-critical equipment at critical locations, the documentation of testing specified by this standard is far too onerous. Therefore, we urge this standard to be made applicable only to the most important facilities and perimeters, such as control centers and energy management systems. A separate, "lite" version of this standard should be made applicable to the remaining equipment standard.</p> <p>SECOND -- The standard should explicitly indicate that it does not apply to "serial" devices.</p> <p>If the first general comment above is not adopted, the opening or introductory paragraph should have something like the following text added:</p> <p>Many of the requirements in this section will not be applicable in the substation environment, since substations are typically unmanned and legacy technology used in them is much more restrictive. Each responsible entity will have to modify or adjust the requirements below to deal with environmental, technical, logistical, personnel, and access differences between such facilities and attended facilities such as control centers or power plants.</p> <p>Add subsection (a)(6) from Section 1301 (revise and renumber format).</p> <p>Consider adding subsection (a)(2)(i)(E) from Section 1302 (if so, revise and renumber format).</p> <p>(a)(1)(2nd parag.) -- Emergency repairs should be excluded from the scope of covered "significant changes."</p> <p>(a)(2) -- The last sentence should have a phrase inserted to</p>	<p>1306 Non-critical cyber assets within the perimeter must be secured to the extent they present a risk to the critical cyber assets.</p> <p>1306 The standard will be enhanced to differentiate between attended and unattended locations.</p> <p>1306.a.01 The drafting team will update the standard to address emergency changes.</p> <p>1306.a.02 The drafting team will update the standard to include requirements for manned and unmanned (i.e. substations, etc.) facilities.</p> <p>1306.a.02 Section 1302 states the requirements for determining critical cyber assets, 1306 applies to all the identified assets in 1302</p> <p>.</p> <p>1306.a.02 The drafting team agrees with your comment and will update the standard accordingly.</p> <p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02 The responsible entity must determine it's own logging strategy that fits the requirement. This strategy must be sufficient to support the investigation of an event and that the integrity of these electronic records is maintained.</p> <p>1306.a.02 The drafting team will update the standard per your comment.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team is in agreement with your</p>

Name	Company	Comments	Responses
		clarify the intent, so that the operative clause reads: "must establish account management practices for all appropriate accounts (e.g., administration, system, generic and guest accounts)."	comments and will revise the draft accordingly.
		(a)(2)(i) -- Implementation of strong passwords may not be possible on legacy equipment. The sentence should read "Where practicable, strong passwords for accounts must be used in the absence of more sophisticated methods such as multi-factor access controls."	1306.a.05 Reference to penetration test removed.
		(a)(2)(ii) -- The phrase "audit trail of the account use" should clarify whether it includes any and all actions while logged on.	1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."
		(a)(2)(iv) -- There is a typo at the end of the third line: "and" should instead be "an."	1306.a.06 Acknowledged – will be done. Thank you.
		(a)(3) -- As proposed, this is impossible to implement for all legacy equipment. In addition, the last sentence is overly prescriptive -- compensating measures are not necessary or possible in every instance. The last sentence should be revised: "Where installation of a patch is not practicable or possible, alternative compensating measures must be evaluated, and that evaluation, as well as any such measures actually taken, must be documented."	1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."
		(a)(4) -- The listed malicious software is inconsistent and not complete -- use a broader term to cover it, such as "malware" (which is included in the list). Revise the subsection to read as follows:  A formally documented process governing the application of anti-malware system integrity tools must be employed to prevent, limit, and/or mitigate their introduction or exposure to critical cyber assets at and within the electronic security perimeter.	1306.a.11 The intent of this requirement is: 1) back-up what you need to in order to recover from any of a range of contingencies; 2) Move a copy far enough away so the same disaster that got the data center doesn't get the back-ups; 3) if the back-up is stored for a prolonged period, test the media periodically to be sure it is still readable should it be necessary to do so. The accepted practice is to conduct random media tests of just a small percentage of the total, selected across the span of the back-up volume. The intent is to determine if the media is failing, so that if the data is important it can be moved to another store as appropriate.
		(a)(5) -- Controlled penetration testing is almost always done by third parties, and is very expensive -- certainly far too expensive and intrusive to require on a yearly basis. Reference to such testing should be removed from the standard and placed -- only as an example -- in the FAQ.	1306.b.01 The drafting team feels a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The drafting team will update the standard to address manned and unmanned facilities (substations, etc.)
		(a)(6) -- Legacy equipment may not be able to generate audit trails. The first sentence should begin with the phrase "Where practicable, critical cyber security assets must generate..."	1306.b.02 The intent of this section is to address mechanics of account and password management on the systems.

Name	Company	Comments	Responses
		<p>(a)(8) -- Delete the phrase "inherent and" -- it is unclear and unnecessary, since it cannot or should not be disabled if used, and if unused is already covered.</p> <p>(a)(11) -- Annual testing is overly burdensome for very large systems, as it is unlikely to have enough benefit to offset the associated costs/inconveniences. In fact, the requirement of any testing may be overly prescriptive, as the issue is broadly ensuring retrievable storage. That may be done by many means that do not lend themselves to testing per se (e.g., at off-site, underground vaults for computer tapes).</p> <p>(b)(1) -- It must be clarified that the test "environment" need not be a separate environment, as long as it is controlled for safety and reliability, especially regarding telecommunications and substation environments that cannot be duplicated to create a "test" environment.</p> <p>(b)(2) --</p> <p>Move the entire subsection to 1303, where it better fits the subject matter, and also reword it to bring it into conformity with that section (revise and renumber format).</p> <p>Clarify that passwords need not be "cracked" to ensure they comply with the policy, but rather that technological or system tools should be used to ensure the required compliance, and that those means should be documented.</p> <p>(b)(3) -- The required "monthly review of all available vender [sic]" patches is over-broad. For instance, users of Solaris V.8 should not have to review patches for V.7. The language should be revised to read: "monthly review of all available and applicable vender" patches.</p>	<p>1306.b.02 The drafting team agrees with your comment and will update the standard accordingly.</p> <p>1306.b.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p>

Name	Company	Comments	Responses
Larry Conrad	Cinergy	<p>1306 -- System Security management</p> <p>While the list of physical controls to be implemented in the proposed section 1305 language represents a huge, solid, and obvious cost burden, requirements in section 1306 represent a less obvious but huge cost burden as well.</p> <p>Once again, there is no evidence presented that there is a relevant threat, which will be mitigated, if these types of controls/documentation requirements are implemented. Also, once again, there is no indication if the idea of associated costs was even contemplated prior to writing the language requiring the controls/documentation.</p> <p>Cinergy requests that evidence needs to be presented showing (1) a relevant threat will be mitigated if the controls outlined in this section are implemented (2) costs and benefits associated with requirements have been identified.</p> <p>Cinergy is concerned that if money and resources are required for documentation requirements that yield no real enhancement to security, then less money and resources will be available for security measures that could truly yield benefit. Recommendation: Either significantly lessen requirements or eliminate many of the following.</p> <p>-- Page 28: Archive backup information for a prolonged period of time and then test it annually to ensure it is recoverable. A definition of 'information' and 'archival information' should be provided. Archived information loses its value in time and may become irrelevant. Is NERC dictating records retention policy? What is the consequence if this does not occur? Requires extra work, but what is the point? Need better understanding of costs vs. benefits.</p> <p>-- Page 28: Create Operating Status Monitoring tools. This section indicates the tools gauge 'performance.' Standard 1300 language contains no statement as to what these performance-monitoring tools are trying to gauge nor are any performance goals indicated. This would be costly to implement with no defined benefit or even goals for the tools. Requires extra work, but what is the point?</p> <p>-- Page 28: Create Operating Status Monitoring tools: Language in the section implies that performance documentation is to be kept for every asset. This is not</p>	<p>1306 The drafting team believes the standards as presented provide a minimum best practices approach to ensuring cyber security.</p> <p>1306.a.01 The intent of the standard is not that every change be documented and tested. The standard states, new systems and SIGNIFICANT changes be tested and documented in a controlled non-production environment. The drafting team will review the standard for consistency.</p> <p>1306.a.01 The intent of the standard is not that every change be documented and tested. The standard states, new systems and SIGNIFICANT changes be tested and documented in a controlled non-production environment. The drafting team will review the standard for consistency.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>1306.a.07 Testing is a subset of Configuration Management. Configuration Management will be moved to section 1301 Governance.</p> <p>1306.a.10 This requirement is about situational awareness of</p>

Name	Company	Comments	Responses
		reasonable.	networked-computing infrastructure deemed to be critical cyber assets. Salient things to monitor can include CPU utilization, memory utilization, running processes, disk partition usage, hung daemons, defunct process queues, line/network throughput, denial of service attacks, and so on. The defined benefit/goal is to be able to tell if systems are operating "normally" in real time, and to know when certain capacity limits are being reached, beforehand. 'Normal' is entirely relative to the systems scenario used by each responsible entity individually.
		-- Page 27: Retention of system Logs: "All critical cyber security assets must generate an audit trail for all security related system events." In the case of local RTU's this is probably not possible.	1306.a.10 That was not the intent. Monitoring is required only for critical cyber assets, as they are defined.
		-- Page 26: Test Procedure language as written is overly burdensome. Language implies that EVERYTHING needs to be tested. It is not realistic that EVERY minor change is documented in formal testing. FAQ's seem to conflict with Std. 1300 proposed language. Recommendation: Modify Standard 1300 language to imply levels similar to NERC's recent Standard 1300 FAQ posting.	1306.a.11 The intent of this requirement is: 1) back-up what you need to in order to recover from any of a range of contingencies; 2) Move a copy far enough away so the same disaster that got the data center doesn't get the back-ups; 3) if the back-up is stored for a prolonged period, test the media periodically to be sure it is still readable should it be necessary to do so. The accepted practice is to conduct random media tests of just a small percentage of the total, selected across the span of the back-up volume. The intent is to determine if the media is failing, so that if the data is important it can be moved to another store as appropriate.
		-- Page 27: Testing "...provide a controlled environment for modifying ALL hardware and software for critical cyber assets." Since the Energy Management System is by nature a critical cyber asset, the language implies that EVERYTHING must be modified in a separate controlled environment. Current language is burdensome and not practical. Recommendation: Indicate a reasonable level for testing within the controlled environment. Use levels similar to those identified in NERC's recent Standard 1300 FAQ posting.	1306.b.01 The drafting team will update the standard to replace potential with known.
		-- Page: 27 Test Procedure Measures: Language states, "...Critical cyber assets were tested for potential security vulnerabilities prior to be rolled into production..." It is unclear what 'potential vulnerabilities' are to be tested or how the tester is to know about them. Recommendation: Explain clearly or delete the reference.	1306.b.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes."
		-- Page 29: Integrity software: Cinergy is pursuing a course of isolating the Energy Management System from the corporate network. This path of isolation reduces threat from email, Internet use, etc. The language requires anti-virus versions be kept immediately up to date. In practice, this conflicts with the work to isolate the EMS and presents un-necessary requirements since the EMS will be isolated from the source of the viruses.	1306.b.04 The standard will be updated to more properly match intent, that a process for governing mitigating of the importation of malicious software into critical cyber assets. It is possible this could be accomplished by isolation.
		-- Page 27: Security Patch Management: Cinergy seeks clarification of "...upgrades to critical cyber assets." If this language includes every upgrade, it is costly and over-burdensome without resulting security benefit.	
		-- Page 27: Created formalized change control & configuration	

Name	Company	Comments	Responses
		<p>management process: Entire section creates un-necessary and redundant requirements that are included in the Test Procedures requirements section of 1306.</p> <p>Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,</p> <ul style="list-style-type: none"> <li>-- Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.</li> <li>-- Patches and upgrades (at the power plant) at Cinergy can only be applied during an outage of the control system.</li> </ul> <p>Cinergy seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?</p> <p>Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, ...no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1301) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>Cinergy recommends:</p> <ul style="list-style-type: none"> <li>- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose</li> </ul>	

Name	Company	Comments	Responses
		<p>a threat...Routine administrative changes ...should be handled within three business days after occurrence."</p> <ul style="list-style-type: none"> <li>- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements within the same Standard.</li> <li>- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.</li> </ul>	



Name	Company	Comments	Responses
Laurent Webber	WAPA	<p>Under 1306(a)(2), please rephrase the second sentence, "The responsible entity must establish...", to make it clear.</p> <p>Reference 1306, System Security Management (b)(2) - Please remove the following from the second sentence in that section "that all accounts comply with the password policy." There is no way to audit whether account passwords comply with the password policy outside of cracking them. The only way to ensure that passwords comply with the password policy is to check for compliance on the front end when the user creates the password.</p>	<p>1306.a.02 The intent of the standard is that the responsible entity will establish policies and procedures for to support the Account Management requirements.</p> <p>1306.b.02 The drafting team agrees with your comment and will update the standard accordingly.</p>

Name	Company	Comments	Responses
Linda Campbell	FRCC	<p>1306 Systems Security Management</p> <p>Change first sentence to: "The responsible entity shall establish a System Security Management Program that minimizes or prevents the risk of failure or compromise from misuse or malicious cyber activity that could affect critical cyber asset(s)."</p> <p>(a) (1) modify sentence 2 to be more clear; Suggestion: Significant changes include security patches, firmware, cumulative service packs, and new release, upgrades, or versions of to operating systems, ...</p> <p>(a) (1) delete the sentence "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment." While this may be a good practice when available, this is not always technically possible. Some systems are so old, there is no way to recreate another similar environment. Also delete, the corresponding wording in the measure (b) (1)</p> <p>(a) (2) (ii) Generic Account Management Revise the last sentence to: "Where individual accounts are not supported or practical in order to maintain critical bulk electric system asset reliability, the responsible entity must have a policy for managing the appropriate use of group accounts that limits access to only those with authorization, an audit trail of the account use, and steps for securing the account in the event of staff changes, e.g., change in assignment or exit."</p> <p>(a) (5) Delete controlled penetration testing- Controlled penetration testing should not be a requirement. These penetration tests (on older generation systems particularly) can cause system outages affecting the reliability of generating units and impacting the very thing we are trying to protect. Each utility should determine which are the best methods of identifying vulnerabilities.</p> <p>(b) (3) and (4) keeping the records related to monthly reviews on the inventory document, may not be the best place to maintain this information. Each utility should be able to determine where this information is retained.</p> <p>(b) (4) Suggest changing last sentence for clarity to -- Where integrity software is not available for a particular computer platform or where other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from</p>	<p>1306 Non-critical cyber assets within the perimeter must be secured to the extent they present a risk to the critical cyber assets.</p> <p>1306.a.01 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.0 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02 The drafting team believes it is important to establish individual accounts where supported.</p> <p>1306.a.05</p> <p>1306.a.10 Monitoring is first and foremost about availability, part of the classic infosec triad of "Confidentiality, Availability, and Integrity"; so indeed monitoring is very much a cyber security issue, by definition...</p> <p>Also, the standard's scope is broader than just "lines," and equally pertains to CPU and disk utilization, for example. As well, periodic test monitoring of low speed serial lines when little change has been introduced to the system is indeed quite a valid approach. However, as we move to more high speed networking in general, with mixed traffic types, real time monitoring is indeed prudent...</p> <p>1306.b.03 The comment is noted.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly</p> <p>1306.b.07 The drafting team agrees and will update the standard accordingly.</p> <p>1306.b.08 The following rewording of 1306.b.08 shall be discussed with the drafting team for possible use in draft 2: "The responsible entity shall disable unused ports and services, and maintain documentation of status/configuration</p>

Name	Company	Comments	Responses
		viruses or and other malicious software, this must also be documented.	of all ports and services available on critical cyber assets.
		(b) (7) The documentation shall verify that all the responsible entity....	1306.b.11 The drafting team agrees with your comment and will update the standard accordingly.
		(b) (8 & 9) -- "against the policy and documented configuration" - what "policy" are you referring to here?	1306.d.02 The drafting team agrees with your comment and will update the standard accordingly.
		(b) (11) modify the end of 1st sentence to -- "... retention schedule of all critical cyber assets' information backup data and tapes."	1306.d.03 Corrected
		(d) (2) and (3) numbered references don't exist in document	
		(e)(2)(ii)(C) Should read "Integrity Software"	
		(e)(3)(iv) Does not mention monthly review measurement.	

Name	Company	Comments	Responses
Linda Nappier	Ameren	1306 (a) (1) Test Procedures: Are OEM tests acceptable to meet this requirement or is each utility expected to perform the security tests?	1306.a.01 If OEM tests effectively test for security vulnerabilities, they are acceptable.

Name	Company	Comments	Responses
Lloyd Linke	WAPA - MAPP	Under 1306 (a) (2), please rephrase the 2nd sentence (The responsible entity must establish...) to make it clear.	1306.a.02 The intent of the standard is that the responsible entity will establish policies and procedures for to support the Account Management requirements.

Name	Company	Comments	Responses
Lyman Schaeffer	Pacific Gas & Electric	<p>1306: Systems Security Management:</p> <p>The same observation cited above applies here as well. It appears that the requirements for password protection and other measures are not based on the lessons derived from the risk assessment performed as part of this process. We believe that such specifics should be worked out as a risk management decision on the part of the company since they're ultimately responsible for the reliability of the system.</p> <p>While we agree with the concept that we must have the process in place for managing default accounts, we believe that the standard does not consider the possibility that certain accounts may not be able to produce audit trails for such accounts. Securing the account in the event of staff changes would be a big burden particularly in a large company where there are many devices and users.</p> <p>This section also requires that we establish a change control process that provides a control environment for modifying all hardware and software for critical cyber assets. Our concern is that a controlled environment should not be interpreted as a separate test environment as this is not always possible particularly when dealing with substation and telecommunication devices. Also, there needs to be some provision for emergency "repairs."</p> <p>This section requires that archival information be stored on computer storage medium and tested at least annually to ensure that it is recoverable. While we agree with this concept, we are concerned that reloading all archival material on an annual basis for a system as large as ours would be very burdensome and probably not worth the effort.</p>	<p>1306.a.02 The responsible entity should document their environment as a compensating measure for mitigating risk if this is the case.</p> <p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>The drafting team feels employees terminated for cause pose a possible threat and should have access rights removed with 24 hours. Routine are given 7 calendar days to allow for normal business processing to remove rights.</p> <p>1306.a.05 The drafting team agrees with your comment and has updated the standard to address unattended facilities.</p> <p>1306.a.06 Acknowledged. All large firms face this, and the accepted procedure is to conduct random media tests of just a small percentage of the total volume, selected across the span of the back-up. The intent is to determine if the media is failing, so that if the data is important it can be moved to another store.</p>

Name	Company	Comments	Responses
Michael Anderson	Midwest ISO	<p>System Logs - Can the requirement for system log retention be made clearer? The requirement appears to be 3 years with a 90 day incident window. How is the 3 years measured? From the start or midpoint of the 90 days?</p> <p>Test Procedures -- Can this section of the document be made to address specific layers of testing? For example the way that this is written I would assume that all Microsoft Windows Patches would have to be applied in a multi-faceted test environment to ensure that there would be no issues.</p> <p>Password/Account Management -- Can the section regarding auditing of user activity be expanded? Most companies have the ability to maintain audits logs at the OS level, however few applications are written with this type of functionality.</p> <p>Security Patch Management -- Can the term "compensating measure" be further explained?</p> <p>Integrity Software -- This section is clear about the need but does not address a requirement for logging or maintaining a patched/unpatched list. Should it?</p> <p>Archived Materials -- Could the requirement of archived materials testing be made clearer? If we are retaining 3 years of data and using a medium like off-line tape it could take a huge amount of time if we must for example completely test all tapes. Does a header check suffice as a sufficient test?</p>	<p>1306.a.01 Each Entity is responsible for determining the appropriate level of testing for their environment. All MS Windows patches are not required to be tested, only cumulative patches that would constitute a significant change.</p> <p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception. The responsible entity must determine it's own logging strategy that fits the requirement. This strategy must be sufficient to support the investigation of an event and that the integrity of these electronic records is maintained. (add this to the FAQ)</p> <p>1306.a.03 See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly</p> <p>1306.a.06 In each case the measure is in 'calendar' days/years. To be updated in draft 2... Wording also to be modified to read: "...3 calendar years from the data of discovery of the incident.</p> <p>1306.a.06 Acknowledged. All large firms face this, and the accepted procedure is to conduct random media tests of just a small percentage of the total, selected across the span of the archive. The intent is to determine if the media is failing, so that if the data is important it can be moved to another store as appropriate.</p>

Name	Company	Comments	Responses
Neil Phinney	Georgia Transmission Co	1306.a.7 This appears to require an audit trail of each access to an RTU and/or communication device. Is that what is intended?	1306.a.07 The draft will be changed to address manned and unmanned substations in this section.
		1306.a.9 Much more detail is required otherwise this is meaningless.	1306.a.9 This comment cannot be addressed without more specific information from the commenter.
		1306.a.10 Although it is good practice to monitor utilization and performance, We don't see the connection to a security issue. It is not clear whether each line needs to be constantly monitored or whether the tools must simply be available on an as-needed basis. To constantly monitor utilization on all lines is not justified.	<p>1306.a.10 Monitoring is first and foremost about availability, part of the classic infosec triad of "Confidentiality, Availability, and Integrity"; so indeed monitoring is very much a cyber security issue, by definition...</p> <p>Also, the standard's scope is broader than just "lines," and equally pertains to CPU and disk utilization, for example. As well, periodic test monitoring of low speed serial lines when little change has been introduced to the system is indeed quite a valid approach. However, as we move to more high speed networking in general, with mixed traffic types, real time monitoring is indeed prudent...</p>



Name	Company	Comments	Responses
Paul McClay	Tampa Electric Company	<p>1306 Systems Security Management</p> <p>Change first sentence to: "The responsible entity shall establish a System Security Management Program that minimizes or prevents the risk of failure or compromise from misuse or malicious cyber activity that could affect critical cyber asset(s).</p> <p>(a) (1) modify sentence 2 to be more clear; Suggestion: Significant changes include security patches, firmware, cumulative service packs, and new release, upgrades, or versions of to operating systems, ..</p> <p>(a) (1) delete the sentence "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment." While this may be a good practice when available, this is not always technically possible. Some systems are so old, there is no way to recreate another similar environment. Also delete, the corresponding wording in the measure (b) (1)</p> <p>(a) (2) (ii) Generic Account Management Revise the last sentence to: "Where individual accounts are not supported or practical in order to maintain critical bulk electric system asset reliability, the responsible entity must have a policy for managing the appropriate use of group accounts that limits access to only those with authorization, an audit trail of the account use, and steps for securing the account in the event of staff changes, e.g., change in assignment or exit.</p> <p>(a) (5) Delete controlled penetration testing- Controlled penetration testing should not be a requirement. These penetration tests (on older generation systems particularly) can cause system outages affecting the reliability of generating units and impacting the very thing we are trying to protect. Each utility should determine what are the best methods of identifying vulnerabilities.</p> <p>(a) (9) This section indicates we shall "secure dial-up-modem connections, but lists no requirements for how to secure dial-up modems."</p> <p>(b) (3) and (4) keeping the records related to monthly reviews on the inventory document, may not be the best place to maintain this information. Each utility should be able to determine where this information is retained.</p>	<p>1306 Non-critical cyber assets within the perimeter must be secured to the extent they present a risk to the critical cyber assets.</p> <p>1306.a.01 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.0 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02 The drafting team believes it is important to establish individual accounts where supported.</p> <p>1306.a.05 In current industry vernacular, use of the term "controlled" in this context distinguishes testing typically conducted internally, where the systems environment is known and potential dangers are controlled-for, versus 'blind' or 'red team' testing. The latter is typically conducted by people who are given no information at the start, with the goal of seeing if security perimeters can be breached by trial and error, brute force, stealth, or masquerade, etc. It is agreed that each responsible entity should determine methods for identifying their own vulnerabilities in a manner appropriate to need and risk. At the same time, however, another part of the 1300 standard requires that all system testing -- upgrades, patches, vulnerability testing, etc. - be conducted only on systems which are not connected to the production environment, in order to preclude adverse impact such as that noted in the comment. In other words, "outage created by either category of penetration testing should be beyond the realm of possibility if the responsible entity is compliant with the rest of the standard.</p> <p>1306.a.09 There are a variety of technical and procedural ways to address this need, and it needs to be addressed. The drafting team cannot specify methods or products, and the responsible entity shall have to decide appropriate measures to protect itself.</p>

Name	Company	Comments	Responses
		(b) (4) Suggest changing last sentence for clarity to -- Where integrity software is not available for a particular computer platform or where other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from viruses or and other malicious software, this must also be documented.	1306.a.10 Monitoring is first and foremost about availability, part of the classic infosec triad of “Confidentiality, Availability, and Integrity”; so indeed monitoring is very much a cyber security issue, by definition...
		(b) (7) The documentation shall verify that all the responsible entity....	Also, the standard’s scope is broader than just “lines,” and equally pertains to CPU and disk utilization, for example. As well, periodic test monitoring of low speed serial lines when little change has been introduced to the system is indeed quite a valid approach. However, as we move to more high speed networking in general, with mixed traffic types, real time monitoring is indeed prudent...
		(b) (8 & 9) -- "against the policy and documented configuration" - what "policy" are you referring to here? And both indicate we need to take "appropriate actions to secure" -- who decides what is "appropriate?"	1306.b.03 The comment is noted.
		(b) (11) modify the end of 1st sentence to "... retention schedule of all critical cyber assets' information backup data and tapes.	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly
		(d) (2) and (3) numbered references don't exist in document	1306.b.07 The drafting team agrees and will update the standard accordingly.  1306.b.08 The following rewording of 1306.b.08 shall be discussed with the drafting team for possible use in draft 2: “The responsible entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on critical cyber assets.  1306.b.11 The drafting team agrees with your comment and will update the standard accordingly.  1306.d.02 The drafting team agrees with your comment and will update the standard accordingly.  1306.d.03 Corrected

Name	Company	Comments	Responses
Pedro Media	FPL	<p>1306 1306 Many of the requirements in this section will not be applicable in the substation environment, since substations are typically unmanned and legacy technology used in them is much more restrictive. Each responsible entity will have to modify or adjust the requirements below to deal with environmental, technical, logistical, personnel, and access differences between such facilities and attended facilities such as control centers or power plants.</p> <p>1306 1306 Also, the Black-Out Report made mention that Computer Forensics capabilities were required for the electric sector. This standard calls for a great deal of documentation and the capability to archive review data for years on out, but makes no mention of forensic processing, proper methods to perform such reviews or the need for companies to have some level of computer forensic capabilities, whether they be in-house or outsourced. We suggest that such a provision be written into the standard at this time and in this section</p> <p>1306. 1306 In general, this section is far too prescriptive in the sense of documentation, and may not be practical for legacy systems. We strongly encourage a complete re-write of this section with thought placed into how documentation intensive said section can become.</p> <p>1306.a.01 1306.a Test procedures should be generic for any type of change and not prescriptive for specific changes, such as patch management, etc. In addition, testing is not always possible or practical in a "isolated environment. Testing of some applications &amp; systems would not be possible in a "isolated test environment." Therefore, we suggest that testing be done in such a manner where the entity has taken reasonable precautions to implement changes on only part of their systems and not all of their critical devices. Said changes would be allowed to operate on the live environment for a predetermined period of time, as determined by that entities test procedures, and replicate on other systems only after sufficient time has elapsed and no malfunctions have occurred.</p> <p>1306.a.01 1306.a.1 Delete the requirement</p> <p>1306.a.02 1306.a.2 Change the first sentence to read "...establish an account password management program, wherever practical and manageable,"</p> <p>1306.a.02 1306.a.2 Change the second sentence to read "...responsible entity must, again wherever practical, establish..."</p> <p>1306.a.02.iii 1306.a.2.iii Change "semiannually" to "annually or as required by security incidents"</p> <p>1306.a.05 1306.a.5 Change the requirement to read "At a minimum, a vulnerability assessment shall be performed at least annually." (Delete the remainder of the requirement.)</p>	<p>1306 Agreed. The draft will be changed to address manned and unmanned substations in this section.</p> <p>1306 Agreed. Requirement a.6 was intended to address this capability.</p> <p>1306. The comment is noted. The drafting team specified a "risk based assessment" because legacy systems may have different security risks and vulnerability resolutions than new systems.</p> <p>1306.a.01 The drafting team is requiring a test procedure. The responsible entity can determine how generic or prescriptive the procedure is to be.</p> <p>The drafting team agrees that some applications can not be tested in an "isolated test environment", the focus of this requirement is security testing and the drafting team believes that security testing can be achieved in an isolated environment.</p> <p>1306.a.01 Noted. This section is being included in section 1301.</p> <p>1306.a.02 Noted. The drafting team feels that it is important to establish an account password management program.</p> <p>1306.a.02 Noted. The drafting team feels that it is important to establish an account password management program</p> <p>1306.a.02.iii The drafting team feels reviews should be conducted more frequently than annually.</p> <p>1306.a.05 Compliance section revised.</p> <p>1306.a.05 Agreed – the drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should most appropriately perform the test.</p> <p>1306.a.07 The drafting team agrees and will update the standard accordingly.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All</p>

Name	Company	Comments	Responses
		<p>1306.a.05 1306.a.5 Penetration tests are not always a recommended review for productions systems. Also who would conduct such a review, a third party vendor or is this assumed to be in-house.</p> <p>1306.a.07 1306.a.7 Change the first sentence to read "The responsible entity shall establish a Change Control Process." Delete the remainder of the sentence.</p> <p>1306.a.08 1306.a.8 Delete "inherent and".</p> <p>1306.a.08 1306.a.8 Add "whenever possible to the end of the sentence"</p> <p>1306.b.01 1306.b.1 Change the measure to "For all critical cyber assets, the responsible entity's change control documentation shall include corresponding records of test procedures", deleting the remainder of the measure.</p> <p>1306.b.02 1306.b.2 Change "quarterly" to "semi-annual".</p> <p>1306.b.02 1306.b.2 Change "5 working days" to "30 working days".</p> <p>1306.b.03 1306.b.3 Change the measure to "The responsible entity's change control documentation shall include a record of all security patch installations in accordance with that entity's patch management policy.", deleting the remainder of the measure.</p> <p>1306.b.04 1306.b.4 Change the measure to "The responsible entity's critical cyber asset inventory and change control documentation shall include a record of all anti-virus, anti-Trojan, and other system integrity tools employed, and the version level actively in use.", deleting the remainder of the measure.</p> <p>1306.b.05 1306.b.5 Change the measure to "The responsible entity shall maintain documentation identifying the organizational, technical and procedural controls, including tools and procedures for monitoring the critical cyber environment for vulnerabilities.", deleting the remainder of the measure.</p> <p>1306.b.06 1306.b.6 Change the first sentence to "The responsible entity shall maintain and retail log files for critical cyber assets.", deleting the remainder of the sentence,</p> <p>1306.b.08 1306.b.8 Change the first sentence to "The responsible entity shall maintain documentation of status/configuration of network services and ports on critical cyber assets.", deleting the remainder of the sentence".</p> <p>1306.b.09 1306.b.9 Change the first sentence to "The responsible entity shall maintain a documented policy for securing dial-up modem connections to critical cyber assets.", deleting the remainder of the sentence.</p> <p>1306.d.01 1306.d Further clarification is required in regards to</p>	<p>other services, including those used for testing purposes, must be disabled prior to production usage.</p> <p>1306.a.08 Declined. The drafting team feels that disabling or uninstalling unused ports and services is an important component of security.</p> <p>1306.b.01 The comment is noted.</p> <p>1306.b.02 Sync up with 1301.5.v (quarterly), and 1305 for quarterly, semi-annual, annual for all reviews</p> <p>1306.b.02 The comment is noted. The drafting team believes the access should be changed sooner than 30 days.</p> <p>1306.b.03 The comment is noted.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.05 The comment is noted.</p> <p>1306.b.06 The drafting team respectfully disagrees. Logs are the basis for audit trails, and logs record "events." An audit trail can and usually is at least in part comprised of event log data. So, it is event logs that must be retained, to support the audit trail. An audit trail can be thought of as (documentation of) a "control process," part of which consists of event logs.</p> <p>1306.b.08 The following rewording of 1306.b.08 shall be discussed with the drafting team for possible use in draft 2: "The responsible entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on critical cyber assets.</p> <p>1306.b.09 This will be raised for discussion by the drafting team for treatment in 1300 draft 2.</p> <p>1306.d.01 The drafting team acknowledges your comment and will address in the FAQs.</p>

Name	Company	Comments	Responses
		"investigations upon complaint." How intrusive are these investigation, and what would predicate such investigations?	

Name	Company	Comments	Responses
Pete Henderson	IMO	<p>1306 Systems Security Management</p> <p>(a) Requirements (1) Test Procedures: The sentence, "Security test procedures shall require that testing and acceptance be conducted on a controlled non-production environment" should be deleted. In practice, testing cannot always be done on a non-production environment, nor is it always necessary to do so. For instance, under some circumstances testing can be done without disrupting normal production by performing the tests on otherwise redundant environment components which are still, strictly speaking, "in production".</p> <p>Futhermore, testing cannot always be done without risk. The final sentence of this sub-section should be modified to read, "All testing must be performed in a manner that precludes, or minimizes, the risk of adversely affecting the production system and operation."</p> <p>(a) Requirements (3) - Security Patch Management Delete the phrase "and configuration management" as it is redundant given the first sentence and the remainder of the sub-section.</p> <p>(a) Requirements (7) - Change Control and Configuration Management Delete reference to Configuration Management in the title as the subsequent text identifies no requirements in this area.</p> <p>(a) Requirements (8) - Disabling Unused Network Ports/Services The reference to "inherent services" is confusing and requires clarification or deletion.</p> <p>(b) Measures (1) - Test Procedures The requirement in 1306 (a) (1) is to mitigate risk from known vulnerabilities. Therefore, in the final sentence of 1306 (b) (1), the word "potential" should be replaced by "known".</p> <p>Delete the words, "on a controlled non-production system" as comments elsewhere.</p> <p>(b) Measures (4) - Integrity Software Delete the words "or" and "also" from the final sentence.</p> <p>(b) Measures (7) - Change Control and Configuration Management Delete the word "all" from the final sentence. As above in</p>	<p>1306.a.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The entity is responsible for determining what is non-production for their environment. It is possible, depending on the entity's environment that redundant components could be considered non-production.</p> <p>1306.a.02 The drafting team believes testing should not pose risk to production operations. The responsible entity should determine the acceptable risk for their operating environment.</p> <p>1306.a.03 The drafting team is in agreement with your comment. It is stated this way because not everyone looks at software updates in the same manner.</p> <p>1306.a.07 Configuration Management will be moved to section 1301 Governance.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.b.01 The drafting team agrees and will update the standard accordingly.</p> <p>1306.b.01 The drafting team feels a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.07 The drafting team agrees and will update the standard accordingly.</p> <p>The drafting team acknowledges your comments and this topic will be addressed as a governance item covered in section 1301.</p> <p>1306.e.01 The drafting team will review the standard and clarify the compliance levels.</p> <p>1306.e.03 The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
		<p>Requirements (7) delete reference to Configuration Management in the title as the subsequent text identifies no requirements in this area</p> <p>(e) Levels of Noncompliance</p> <p>(1) Level One</p> <p>The requirement in 1306 (e) (1) (ii) requires clarification or deletion. The Measures in 1306 do not specify the need to update documentation, and in some cases (eg. passwords) the requirement is to document quarterly, not annually.</p> <p>(3) Level Three</p> <p>The wording of (ii) is confusing and requires clarification</p> <p>Sub-section (3) (iii) (A) appears to specify that failure to perform a quarterly audit of password compliance with policy is a level 3 non-compliance, where as 1306 (e) (2) (ii) (A) states that it is a level 2 non-compliance.</p> <p>The reference to 5.3.3.2 is confusing and should be corrected or deleted.</p>	

Name	Company	Comments	Responses
Phil Sobol	SPP CIPWG	<p>- Testing of changes made to systems should only be required for hardware or software that could have an impact on security. If a software patch has nothing to do with the security of the system, then it should not be required to undergo security test procedures. Only changes that have to do with the OS, user access, etc, should be tested.</p> <p>- Are there anti-virus, anti-Trojan, or other integrity tools, and automatic monitoring tools for all systems? What if there are none for your type of system?</p> <p>- How do you handle changes that have to be made on the spot due to some bug or problem in software that could bring down a system? We need to be able to make these changes quickly; we cannot stop and request permission to make these changes, test them, document them, etc.</p> <p>1306.a.1 paragraph 2 -- This listing is not all inclusive. Re-word as "Significant changes include but are not limited to..." There is no mention of Virus protection. We would strive to be more generic in the wording in order to leave room for new technologies that are not included in this listing.</p> <p>1306.a.1 paragraph 3 -- If the vendor tests patches before sending them to the utility (these are patches related to control of the BES not Microsoft patches), can their documentation and verification that the patch is not going to break the system suffice for internal testing? In the past, we have relied on our vendors to provide patches and updates that work.</p>	<p>1306.a.01 The drafting team believes that patches should be tested to verify they have no impact on security controls.</p> <p>1306.a.01 The drafting team agrees and will revise the standard accordingly.</p> <p>1306.a.01 The intent of the standard is that security testing be conducted. The standard is not addressing functionality testing. If the vendor tests include security testing, are documented, and sufficiently test for the entity's environment they could be deemed acceptable. The drafting team is requiring a test procedure. The responsible entity can determine how what the procedure is to be.</p> <p>1306.a.03 Legacy systems may satisfy the risk based assessment criteria simply by their limited physical access and isolation from the Internet and corporate networks. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.07 Configuration Management will be moved to section 1301 Governance.</p> <p>The entity should include a process for addressing these type situations in their change management policy.</p>



Name	Company	Comments	Responses
Ray A'Brial	CHGE	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>(a)(2) -- The last sentence should have a phrase inserted to clarify the intent, so that the operative reads: "must establish end-user (e.g., administration, system, and guest) account management practices."</p> <p>(a)(2)(i) -- Implementation of strong passwords may not be possible on legacy equipment. The sentence should read "Where practicable, strong passwords for accounts must be used in the absence of more sophisticated methods such as multi-factor access controls."</p> <p>1306.a.2.ii change pooding and puffing to putting (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove Generic from the title</p> <p>1306.a.2.iii, use at least annually instead of at least semi-annually</p> <p>Change 1306.a.3 -- As proposed, this is impossible to implement for all legacy equipment. In addition, the last sentence is overly prescriptive -- compensating measures are not necessary or possible in every instance. The last sentence should be revised: Where installation of a patch is not practicable or possible, alternative compensating measures must be evaluated, and that evaluation, as well as any such measures actually taken, must be document.</p> <p>Remove the last sentence in 1306.a.3, In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented.</p> <p>Change 1306.a.4 -- The listed malicious software is not complete -- use a broader term to cover it, such as mal-ware.</p> <p>(a)(5) -- Controlled penetration testing is almost always done by third parties, and is very expensive -- certainly far too expensive</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		and intrusive to require on a yearly basis. Reference to such testing should be removed from the standard and placed -- only as an example -- in the FAQ.	
		1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).	
		Change 1306.a.6 to	
		Legacy equipment may not be able to generate audit trails. The first sentence should begin with the phrase Where practicable, critical cyber security assets must generate...	
		1306.a.7 Remove Configuration Management from the title	
		1303.a.8 Remove the word inherent it is not clear what is meant by it.	
		1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.	
		1306, remove 1306.a.11 since 1308 addresses back-up and recovery.	
		1306.b.1, remove Test procedures must also include full detail of the environment used on which the test was performed. Also replace potential with known in the last sentence. Also in the last sentence insert the words if possible at the end of the sentence.	
		1306.b..2. -- Move the entire subsection to 1303, and reword to bring it into conformity with that section.	
		1306.b.3, remove;	
		The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels.	
		and change	
		The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset	

Name	Company	Comments	Responses
		<p>compromise from a known vulnerability.</p> <p>to</p> <p>The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability.</p> <p>1306 b.3 first sentence-eliminate the word management.</p> <p>1306.b.4, remove anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change          ..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware.          to          ..mitigate risk of malicious software.</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;</p> <p>Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented.</p> <p>1306.b.5 remove the first sentence.          Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;          The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets.          to          Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis.</p>	

Name	Company	Comments	Responses
		1306.b.7 In the final sentence remove the word all and change the heading by deleting and Configuration Management	
		Remove 1306.b.11, since 1306.a.11 was removed.	
		1306.d.2, change from The compliance monitor shall keep audit records for three years. to The compliance monitor shall keep audit records for three calendar years.	
		1306.d.3.iii, change system log files to audit trails	
		1306.e.2, change the monthly/quarterly reviews to the reviews	
		1306.e.2.ii.C, change anti-virus to malicious	
		1306, the Compliance levels should be updated to match the above measures.	

Name	Company	Comments	Responses
Ray Morella	First Energy	<p>Section 1306 Security Patch Management section presents additional problems for power plant control systems. For example,</p> <ul style="list-style-type: none"> <li>-- Security Patch Management language (page 27) requires timely installation of applicable security patches and operating system upgrades.</li> <li>-- Patches and upgrades (at the power plant) at ABC can only be applied during an outage of the control system.</li> </ul> <p>ABC seeks clarification from NERC as to how all of Section 1306, including Security Patch Management, applies to power plant control systems. Will plants be expected to create more outages to keep up with requirements?</p> <p>Page 28 (2) Account Management: "review access permissions within 5 working days. For involuntary terminations, ...no more than 24 hours". By creating redundant requirements within the same standard, the 1300 language conflicts from one section to the next. (Note: Same comments made in section 1303 &amp; 1301) Need clarification &amp; consistency from NERC on exactly WHAT the access change requirements are.</p> <ul style="list-style-type: none"> <li>- 1301 states: "Responsible entities shall... ensure that modification, suspension, and termination of user access to Critical Cyber Assets is accomplished with 24 hours of a change in user status."</li> <li>- 1303 (ii) (page 14) states "The Responsible entity shall review the document (list of access)... and update listing with in 2 days of a 'substantive change' of personnel." No definition of 'substantive change' was provided.</li> <li>- 1303 (iii) (page 14) states "Access revocation must be completed with 24 hours for personnel who...are not allowed access...(e.g. termination, suspension, transfer, requiring escorted access, etc.)." This implies the time requirement may be different for other changes.</li> <li>- 1306 (p. 28 Account Management Section) says upon normal movement out of the organization, management must review access permissions within 5 working days. For involuntary terminations...24 hours.</li> </ul> <p>ABC recommends:</p> <ul style="list-style-type: none"> <li>- The requirement should be defined as recommended by NERC above 'access should be suspended no later than 24 hours for persons who have exhibited behavior suggesting that they pose a threat...Routine administrative changes ...should be handled within three business days after occurrence."</li> <li>- The requirement should only be defined in one section of the document rather than creating multiple conflicting requirements</li> </ul>	<p>1306.a.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. . The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. . The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The intent of the standard to ensure persons no longer in a job function do not have access to data and/or systems associated with that job function. The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 A review of the standard will be conducted for consistency between sections. . The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.02 A review of the standard will be conducted for consistency between sections. . The standard will be revised to state" "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p>

Name	Company	Comments	Responses
		<p>within the same Standard.</p> <p>- If the requirement is used in the non-compliance section, then the non-compliance section should be consistent with revised requirements.</p>	

Name	Company	Comments	Responses
Richard Engelbrecht	Rocheste Gas & Electric	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p> <p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24</p>	



Name	Company	Comments	Responses
		hours for cause, or seven days".	
		1306.b.3, remove;	
		"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vendor security patches/OS upgrades and current revision/patch levels."	
		and change	
		"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."	
		to	
		"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."	
		1306 b.3 first sentence-eliminate the word "management".	
		1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.	
		1306.b.4 third sentence Change	
		"..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."	
		to	
		"..mitigate risk of malicious software".	
		1306.b.4 Remove the second sentence.	
		1306.b.4 Replace the fourth sentence with;	
		"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."	

Name	Company	Comments	Responses
		<p>1306.b.5 remove the first sentence.</p> <p>Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;</p> <p>"The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p> <p>to</p> <p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"</p> <p>Remove 1306.b.11, since 1306.a.11 was removed.</p> <p>1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."</p> <p>1306.d.3.iii, change "system log files" to "audit trails"</p> <p>1306.e.2, change "the monthly/quarterly reviews" to "the reviews"</p> <p>1306.e.2.ii.C, change "anti-virus" to "malicious"</p> <p>1306, the Compliance levels should be updated to match the above measures.</p>	

Name	Company	Comments	Responses
Richard Kafka	PEPCO	<p>Definition (Section 1306.a.8): What is meant by Inherent services?</p> <p>Section 1306.a.2.i: Existing hardware is grandfathered for password strength by the phrase, ...to the extent allowed by the existing environment. To what extent is other equipment grandfathered, such as logging capability of dial-up equipment and the ability to display an appropriate use banner?</p>	<p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception. The intent of the standard is not to allow a grandfather clause. The intent is to establish a minimum level of password strength.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage.</p>

Name	Company	Comments	Responses
Robert Pelligrini	United Illuminating	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".</p> <p>1306.b.3, remove;</p> <p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p>	

Name	Company	Comments	Responses
		<p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change          "...so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."          to          "...mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;          "Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence.          Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;          "The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."          to</p>	

Name	Company	Comments	Responses
		<p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."</p>	
		<p>1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"</p>	
		<p>Remove 1306.b.11, since 1306.a.11 was removed.</p>	
		<p>1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."</p>	
		<p>1306.d.3.iii, change "system log files" to "audit trails"</p>	
		<p>1306.e.2, change "the monthly/quarterly reviews" to "the reviews"</p>	
		<p>1306.e.2.ii.C, change "anti-virus" to "malicious"</p>	
		<p>1306, the Compliance levels should be updated to match the above measures.</p>	

Name	Company	Comments	Responses
Robert Strauss	NYSEG	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p>	Please see responses to A. Ralph Rufrano.



Name	Company	Comments	Responses
		<p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".</p> <p>1306.b.3, remove;</p> <p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p>	

Name	Company	Comments	Responses
		<p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change  "..so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."  to  "..mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;</p> <p>"Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence.  Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;  "The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."</p>	

Name	Company	Comments	Responses
		to "Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."	
		1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"	
		Remove 1306.b.11, since 1306.a.11 was removed.	
		1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."	
		1306.d.3.iii, change "system log files" to "audit trails"	
		1306.e.2, change "the monthly/quarterly reviews" to "the reviews"	
		1306.e.2.ii.C, change "anti-virus" to "malicious"	
		1306, the Compliance levels should be updated to match the above measures.	

Name	Company	Comments	Responses
Roman Carter	Southern Company	<p>1306 (Systems Security Management)</p> <p>-- In (a)(2)(iv), the standard requires auditing of all account usage to an individual person. It is questionable as to whether all 'cyber assets' are capable of this if the asset only has one device-level password. In Unix parlance this implies using a "su to root" technique. In many cases, this is not possible and it is necessary for administrative or root accounts to be used directly.</p> <p>-- In (a)(3), the standard states that in the case where a patch installation is not possible, a compensating measure MUST be taken and documented. This assumes that a compensating measure is ALWAYS available and can be implemented, which may not be the case.</p> <p>-- In (a)(5), it states at a minimum, at least annually a 'controlled penetration test' must be conducted against the access points of the electronic perimeter. Again, this may not scale to thousands of perimeters. Clarification is also needed as to what constitutes a 'controlled penetration test' as that is an ambiguous term. Scanning for open ports/services has proven to be disruptive and even fatal to the production operation of some critical systems and cannot be routinely applied to all internal control networks. Penetration testing and scanning at the access points would be acceptable.</p> <p>-- In (a)(6), the standard requires that all cyber assets must generate an audit trail and must be retained for 90 days. Are all devices capable of this? Also, what is an 'exportable' format? -- 1306(a)(10) "Computer and communications systems used for operating critical infrastructure must include or be augmented with automated tools to monitor operating state, utilization, and performance, at a minimum." These are operational and not cyber-security issues and do not belong in this standard.</p> <p>-- 1306(b)(1) "For all critical cyber assets, the responsible entity's change control documentation shall include corresponding records of test procedures, results, and acceptance of successful completion." Does this apply only to security-related test and procedures as implied by 1306(a)(1) or all changes including functional and hardware? If all changes, this is out of the scope of this requirement. If just security-related changes then that need clarification in this measurement.</p> <p>-- 1306(b)(1) "Test procedures must also include full detail of the environment used on which the test was performed." The test environment for a specific critical cyber asset should be documented and then referenced in the test procedures rather re-documented in every instance of the test procedures.</p> <p>-- 1306(b)(3) "The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vendor patches/OS upgrades and current</p>	<p>1306.a.02.iv The intent of the standard is that an individual person is associated with the account and manages access to the account by other individuals. The responsible entity should document this individual and all individuals with access to the generic account.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.06 Certainly not all devices are capable of generating extensive logs. However, for example, it's possible to maintain a manual log of configuration changes made over time to a so-defined critical RTU or relay. Each responsible entity will have to look at what is appropriate to monitor for each cyber asset deemed to be critical, and implement some way to do so. Where equipment cannot generate logs at all, it may not be possible to do more than manually record configuration or maintenance changes manually made. If the equipment does not provide digital logs, so be it. Next time, buy equipment that does... "Exportable" typically means tab-delimited, space-delimited, comma delimited, flat-file, or similar.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.a.09 This will be raised for discussion by the drafting team for treatment in 1300 draft 2.</p> <p>1306.a.10 Monitoring is first and foremost about availability, part of the classic infosec triad of "Confidentiality, Availability, and Integrity"; so indeed monitoring is very much a cyber security issue, by definition... This requirement is about "situational awareness" of networked-computing infrastructure, and each responsible entity will have to figure</p>

Name	Company	Comments	Responses
		<p>revision/patch levels. The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability." First, the wording does not limit OS upgrades to cyber-related vulnerability mitigation. The current wording is "all." Secondly, even for cyber-related patches, monthly application of vendor patches/OS upgrades and current revision/patch levels is not realistic for most SCADA/EMS systems and other systems that are tightly coupled to their OS and third party applications. Security patches/OS upgrades and implementation of third party application release upgrades cannot be applied without extensive testing and often code changes and usually require the close involvement of the original system vendor. Quarterly review of security patches, OS upgrades, etc. and a planned risk-based mitigation strategy to implement those patches, upgrades, etc. based on vendor recommendations should be followed.</p> <p>-- 1306(b)(4) "Integrity Software" This section is written from a "Windows-centric" perspective. As noted, anti-virus tools are not available for many of the critical cyber security platforms and as such the intent of this section does not apply.</p> <p>-- 1306(b)(5) "The documentation will also include a record of the annual vulnerability assessment, and remediation plans for all vulnerabilities and/or shortcomings that are found. The documentation shall verify that the responsible entity is taking appropriate action to address the potential vulnerabilities." There are always "vulnerabilities". There has to be a risk-based cost benefit trade-off mitigation strategy to determine which vulnerabilities should be addressed. It is naive to think that all potential vulnerabilities can or should be addressed. The language of the standard should address vulnerability remediation from a risk-based cost benefit approach.</p> <p>-- 1306(b)(8) "The responsible entity shall maintain documentation of status/configuration of network services and ports on critical cyber assets, and a record of the regular audit of all network services and ports against the policy and documented configuration." The standard should contain language along the lines of "the responsible entity will follow vendor recommendations for securing network services and ports on critical cyber assets"; in general, the system vendor must identify which network services and ports that can be disabled.</p> <p>-- 1306(b)(10) "Operating Status Monitoring Tools: The responsible entity shall maintain a documentation identifying organizational, technical, and procedural controls, including</p>	<p>out for itself how it will establish and maintain situational awareness for its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>1306.a.10 Monitoring is first and foremost about availability, part of the classic infosec triad of "Confidentiality, Availability, and Integrity"; so indeed monitoring is very much a cyber security issue, by definition... This requirement is about "situational awareness" of networked-computing infrastructure, and each responsible entity will have to figure out for itself how it will establish and maintain situational awareness for its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>1306.b.01 The intent of the standard is to document test procedures. The drafting team will update the standard to clarify.</p> <p>1306.b.01 The drafting agrees and will update the standard accordingly.</p> <p>1306.b.01 The testing environment should be documented to ensure it adequately represents the production environment and security testing.</p> <p>1306.b.02 The drafting team will review the standard for consistency.</p> <p>1306.b.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application or frequent upgrades are not practical, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p>

Name	Company	Comments	Responses
		<p>tools, and procedures for monitoring operating state, utilization, and performance of critical cyber assets." These are operational issues and not cyber-security issues and do not belong in this standard.</p> <p>-- 1306(e)(1)(i) "Document(s) exist, but have does not cover ..." Delete the word "have".</p> <p>-- 1306(e)(2)(ii)B) "Security Patch Management (monthly)" See comment to 1306(b)(3) above. Monthly patch management review is too frequent to be practical.</p> <p>-- 1306(e)(3)(iii)B) Reference 5.3.3.2 should be deleted.</p> <p>-- 1306(e)(3)(vi)B) "Documentation verifying that the entity is taking appropriate actions to remediate potential vulnerabilities does not exist." See comment to 1306(b)(5) above. The language of the standard should address vulnerability remediation from a risk-based cost benefit approach.</p> <p>-- 1306(e)(3)(ix) "Change Control and Configuration Management: N/A" This should be spelled out as to the specific issue, e.g., change control and configuration management documentation does not exist.</p> <p>-- 1306(e)(3)(x) "Operating Status Monitoring Tools: N/A" This is not a cyber-security issue and does not belong in this standard.</p> <p>-- In (a)(8), delete the 'inherent and'. You should disable all unused services, whether they are inherent or not, and some inherent services are vital.</p> <p>-- Delete (a)(9), which simply states "The responsible entity shall secure dial-up modem connections". This is an electronic perimeter item and should be covered there, not in 1306.</p> <p>-- Consider deletion of (a)(10) which calls for tools to monitor operating state, utilization, and performance, at a minimum. These are not security oriented functions and should not be requirements of a cyber security standard.</p> <p>-- In (b)(1), please clarify what 'Test procedures must also include full detail of the environment used on which the test was performed' means.</p> <p>-- In (b)(2), delete the access permissions review statements as they are covered in the Personnel standard and do not need to be duplicated here.</p>	<p>1306.b.05 Agreed – the drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should most appropriately perform the test.</p> <p>1306.b.08 The following rewording of 1306.b.08 shall be discussed with the drafting team for possible use in draft 2: "The responsible entity shall disable unused ports and services, and maintain documentation of status/configuration of all ports and services available on critical cyber assets." One would presume that the entity would consult vendors as to ports used for application processing before disabling any.</p> <p>1306.b.10 Monitoring is first and foremost about availability, part of the classic infosec triad of "Confidentiality, Availability, and Integrity"; so indeed monitoring is very much a cyber security issue, by definition... This requirement is about "situational awareness" of networked-computing infrastructure, and each responsible entity will have to figure out for itself how it will establish and maintain situational awareness for its set of critical cyber assets in operation. Inadequate situational awareness was a finding from the investigation of the NE blackout of 2003.</p> <p>1306.e.01.i The drafting team agrees and will update the standard accordingly.</p> <p>1306.e.02.ii.B The intent is that the responsible entity has an awareness of published vulnerabilities and vendor available patches.</p> <p>1306.e.03.iii.B The compliance measures will be reviewed and revised accordingly.</p> <p>1306.e.03.ix The compliance measures will be reviewed and revised accordingly.</p> <p>1306.e.03.vi.B The compliance measures will be reviewed and revised accordingly.</p> <p>1306.e.03.x The compliance measures will be reviewed and revised accordingly.</p>

Name	Company	Comments	Responses
S. Kennedy Fell	NYISO	<p>In 1306.a.1, last paragraph, modify the second sentence to read as follows;</p> <p>"Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment if possible."</p> <p>1306.a.2.ii change "pooding" and "puffing" to "putting" (it appears a pdf translation problem as some documents the group printed have it and others did not)</p> <p>1306.a.2.ii remove "Generic" from the title</p> <p>1306.a.2.iii, use "at least annually" instead of "at least semi-annually"</p> <p>Change 1306.a.3 from;</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches and upgrades to critical cyber security assets."</p> <p>to</p> <p>"A formal security patch management practice must be established for tracking, testing, and timely installation of applicable security patches to critical cyber security assets." (NPCC believes that it upgrades are a subset of the applicable security patches.)</p> <p>Remove the last sentence in 1306.a.3, "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented."</p> <p>Change 1306.a.4 from;</p> <p>"A formally documented process governing the application of anti-virus, anti-Trojan, and other system integrity tools must be employed to prevent, limit exposure to, and/or mitigate importation of email-based, browser-based, and other Internet-borne malware into assets at and within the electronic security perimeter."</p> <p>to</p> <p>"A formally documented process governing mitigation of the importation of malicious software into critical cyber assets."</p> <p>1306.a.6, request that the logs be defined (e.g. operator, application, intrusion detection).</p>	Please see responses to A. Ralph Rufrano.

Name	Company	Comments	Responses
		<p>Change 1306.a.6 from</p> <p>"All critical cyber security assets must generate an audit trail for all security related system events. The responsible entity shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved for a period three (3) years in an exportable format, for possible use in further event analysis."</p> <p>to</p> <p>"It must be possible to create an audit trail for all security incidents affecting critical cyber assets. In the event of a security incident affecting a critical cyber asset said audit trail must be preserved for three calendar years in an exportable format, for possible use in further event analysis."</p> <p>1306.a.7 Remove "Configuration Management" from the title</p> <p>1303.a.8 Remove the word "inherent" it is not clear what is meant by it.</p> <p>1306.a.10 needs clarification. What are we monitoring? What is the purpose of the monitoring tools? Please either clarify the intent or remove.</p> <p>1306, remove 1306.a.11 since 1308 addresses back-up and recovery.</p> <p>1306.b.1, remove "Test procedures must also include full detail of the environment used on which the test was performed." Also replace "potential" with "known" in the last sentence. Also in the last sentence insert the words "if possible" at the end of the sentence.</p> <p>1306.b.2, instead of "24 hours" use the above wording on "24 hours for cause, or seven days".</p> <p>1306.b.3, remove;</p> <p>"The responsible entity's critical cyber asset inventory shall also include record of a monthly review of all available vender security patches/OS upgrades and current revision/patch levels."</p> <p>and change</p>	



Name	Company	Comments	Responses
		<p>"The documentation shall verify that all critical cyber assets are being kept up to date on OS upgrades and security patches or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known vulnerability."</p> <p>to</p> <p>"The documentation shall verify that all critical cyber assets are being kept up to date on Operating System upgrades and security patches that have been verified applicable and necessary or other compensating measures are being taken to minimize the risk of a critical cyber asset compromise from a known security vulnerability."</p> <p>1306 b.3 first sentence-eliminate the word "management".</p> <p>1306.b.4, remove "anti-virus, anti-Trojan, and other" from the first sentence.</p> <p>1306.b.4 third sentence Change          "...so as to minimize risk of infection from email-based, browser-based, or other Internet-borne malware."          to          "...mitigate risk of malicious software".</p> <p>1306.b.4 Remove the second sentence.</p> <p>1306.b.4 Replace the fourth sentence with;          "Where integrity software is not available for a particular computer platform, other compensating measures that are being taken to minimize the risk of a critical cyber asset compromise from viruses and malicious software must also be documented."</p> <p>1306.b.5 remove the first sentence.          Based on the common use of third parties for outsourcing of this associated work of vulnerability assessment, it is not reasonable to maintain the information called for in sentence one.</p> <p>Change 1306.b.6 from;          "The responsible entity shall maintain documentation that index location, content, and retention schedule of all log data captured from the critical cyber assets. The documentation shall verify that the responsible entity is retaining information that may be vital to internal and external investigations of cyber events involving critical cyber assets."          to</p>	

Name	Company	Comments	Responses
		<p>"Responsible entity shall maintain audit trail information for all security incidents affecting critical cyber assets for three calendar years in an exportable format, for possible use in further event analysis."</p>	
		<p>1306.b.7 In the final sentence remove the word "all" and change the heading by deleting "and Configuration Management"</p>	
		<p>Remove 1306.b.11, since 1306.a.11 was removed. 1306.d.2, change from "The compliance monitor shall keep audit records for three years." to "The compliance monitor shall keep audit records for three calendar years."</p>	
		<p>1306.d.3.iii, change "system log files" to "audit trails"</p>	
		<p>1306.e.2, change "the monthly/quarterly reviews" to "the reviews"</p>	
		<p>1306.e.2.ii.C, change "anti-virus" to "malicious"</p>	
		<p>1306, the Compliance levels should be updated to match the above measures.</p>	

Name	Company	Comments	Responses
Scott McCoy	Xcel Energy	Under 1306 (a) (2), please rephrase the 2nd sentence (The responsible entity must establish...) to make it clear.	1306.a.02 The intent of the standard is that the responsible entity will establish policies and procedures for to support the Account Management requirements.

Name	Company	Comments	Responses
Seiki Harada	BC Hydro	<p>1306 System Security Management describes Security Patch Management. This section talks about tracking of all patches applied. These are necessary actions. However, in order to make this management process complete, there should be a log of ALL pertinent security patches published by respective software manufacturers, or all published vulnerabilities regardless of the availability of patches from the manufacturer, and their disposition. . An entity may accept some of these as a reasonable risk to take and do nothing except to log the decision, while others will take some defensive measures and require being logged. The evaluation results and the management decision/disposition should be logged in all cases.</p> <p>Still on the same section, there is a requirement for "Backup and Recovery". These are again necessary functions. In addition, though, there must be a viable "disaster response plan" ready and maintained in case of a major catastrophe that may render mere backup and recovery irrelevant.</p>	<p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p>

Name	Company	Comments	Responses
Stacy Bresler	Pacificorp	<p>1306.a.1 This puts the entity on the hook for understanding the security architecture of applications -- by what industry standard does the lowly tech at a generation plant check a script change to a Siemens EMS? Do they realize how big of an animal this could be? I can appreciate the intention, but the onus for application security of commercial apps should be on the vendor. I'd like to see a distinction between in-house system administrative and operational configuration changes, and the commercial vendor changes relative to the requirement for evaluating with formal information security checklists.</p> <p>1306.a.2.i As conditions of a "strong password", alpha, numeric and special characters were mentioned as complexity criteria. Please include a required or recommended password length as well.</p> <p>1306.a.2.i "...to the extent allowed by the existing environment." -- this will be an open loophole for all legacy systems that cannot enforce password complexity requirements. Additionally, it is unclear whether or not "allowed" is intended to indicate policy-based or technology-based restrictions. It should clearly state that, if the technology allows, then the policy cannot be less restrictive and should enforce all required password complexity requirements within the standard.</p> <p>1306.a.4 "Integrity Software" -- this terminology is inconsistent with traditional usage within the Information Security lexicon. This would usually indicate software such as TripWire, Intact, or other file/registry hashing tools. The context provided is more aligned with AntiVirus or malicious code prevention software. Please consider replacing the "Integrity" with "AntiVirus" or other more appropriate term.</p> <p>1306.a.5 Running certain tools (such as NMAP) may cause severe system instability or even denial of service within Process Control environments. It should be stated that NERC is not recommending that controlled penetration testing be performed within the PCS environment, rather only at the point of ingress/egress.</p> <p>1306.a.8 "...disable inherent and unused services." -- consider revising this to state that only those services explicitly required for normal and emergency operations are allowed. All other services, including those used for testing purposes, must be disabled prior to production usage.</p> <p>1306.a.9 "... secure dial-up modem connections." -- please provide minimum requirements, such as those provided in the "Securing Remote Access to Electronic Control and Protection Systems" Guideline (<a href="http://www.esisac.com/publicdocs/Guides/secguide_pcs_final.p">http://www.esisac.com/publicdocs/Guides/secguide_pcs_final.p</a></p>	<p>1306.a.01 The drafting team believes outsourcing does not relieve management of fiduciary oversight responsibility. If the vendor tests include security testing, are documented, and sufficiently test for the entity's environment they could be deemed acceptable.</p> <p>1306.a.02.i The drafting team agrees with your comment and will update the standard accordingly.</p> <p>1306.a.02.i The drafting team agrees with your comment and will update the standard accordingly.</p> <p>1306.a.04 The drafting team understands your comment, however believes that the use of "Integrity Software" in a manner consistent with the standard is gaining use. See FAQ for further clarification.</p> <p>1306.a.05 The drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should most appropriately perform the test.</p> <p>1306.a.08 The following alternate language will be applied in 1300 draft 2: "The responsible entity shall enable only those services required for normal and emergency operations. All other services, including those used for testing purposes, must be disabled prior to production usage."</p> <p>1306.a.09 The standard should only state that they must be secured. The noted reference along with many other sources offer potential approaches to doing so and can be consulted by responsible entities as they may wish.</p> <p>1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.b.10 standard will be revised.</p>

Name	Company	Comments	Responses
		<p>df)</p> <p>1306.b.4 As stated above in ID 12, "Integrity Software" -- this terminology is inconsistent with traditional usage within the Information Security lexicon. This would usually indicate software such as TripWire, Intact, or other file/registry hashing tools. The context provided is more aligned with AntiVirus or malicious code prevention software. Please consider replacing the "Integrity" with "AntiVirus" or other more appropriate term.</p> <p>1306.b.4 ...Internet-borne malware." -- not all malware is Internet-borne. Please consider revising to include all malware.</p> <p>1306.b.10 "...shall maintain a documentation identifying..." is grammatically incorrect. Please revise the sentence to read "...shall maintain a document identifying..."</p>	

Name	Company	Comments	Responses
Terry Doern	BPA	<p>1306.a.1 BPA Transmission is in agreement with the WECC EMS WG's comment: Remove "Security test procedures shall require that testing and acceptance be conducted on a controlled nonproduction environment." The last sentence is an adequate statement.</p> <p>1306.a.2 It has been our experience that having "Strong" passwords is not a measure of protection. Protecting the password files themselves is more valuable than having strong passwords. Strong passwords merely slow down unauthorized access a bit.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: Should qualify "strong password" as to where it is technically supported. Not all technology allows for this.</p> <p>Access Reviews is covered within other sections of this standard. Should be reconciled to ensure consistency.</p> <p>1306.a.3 "In the case where installation of the patch is not possible, a compensating measure(s) must be taken and documented." This is too restrictive. It conflicts with "applicable" in 1st sentence.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: The word 'timely' does not adequately reflect the risk management approach that should be used in applying patches. 1306.a.4 BPA Transmission is in agreement with the WECC EMS WG's comment: Needs to state that it will exist "where applicable as defined by the entity".</p> <p>1306.a.6 BPA Transmission is in agreement with the WECC EMS WG's comment: The first sentence needs to be changed to reflect that audit trails need to be generated, but not necessarily by the asset as described within the first sentence. Not all devices have this capability. Additionally, should state "where technically feasible".</p> <p>What is the definition of "security related system events"?</p> <p>1306.a.7 BPA Transmission is in agreement with the WECC</p>	<p>1306.a.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities.</p> <p>1306.a.02 The intent of the standard is provide a minimal set of requirements. The responsible entity should provide additional measures when cabable.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team believes a formally documented process governing mitigation of the importation of malicious software into critical cyber assets of some form is applicable to each entity.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>Security Related Events -- This is completely situation-dependent, so the responsible entity will have to create valid audit trails for itself by close examination of processes and procedures in operation. 'Events' are distinguished as being more fundamental than 'incidents'; in fact, the latter is often composed of one or more of the former. Examples of events</p>

Name	Company	Comments	Responses
		<p>EMS WG's comment:</p> <p>This section sound very much like section 1301, authorization to place into production. Should be reconciled to ensure consistency.</p> <p>What is the definition of a "controlled environment"? Could be interrupted as a separate test environment, is this what is intended?</p> <p>1306.a.11 Suggested text - "System backup information should be tested at least annually."</p> <p>Define prolonged period.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment:</p> <p>This section is not about archival, it is about back-up and recovery, so the last sentence should be removed.</p>	<p>are system administrator execution of privileged commands, both successful and unsuccessful, extended failed login attempts, new account creation, configuration changes, and discovery of network port-probing, to name but a few. At the application level, examples could be logs of system re-directs, or logging of attempts to manually modify production data.</p> <p>1306.a.07 Configuration Management will be moved to section 1301 Governance.</p> <p>The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The intent is to provide as much separation as possible from production systems. The entity should determine the appropriate level of separation for their environment.</p> <p>1306.a.11 Suggestion noted. While other compliance requirements incumbent upon a responsible entity (e.g., SOX) may indeed require longer retention periods, there is at least the requirement herein to maintain event logs pertinent to a cyber security incident for three calendar years from the date of discovery. So, prolonged is at least three years. The requirement to conduct random viability tests of the back-up media is to assure that it can still be read three years hence.</p>



Name	Company	Comments	Responses
Tom Flowers	Centerpoint Energy	<p>Page 26, 1306 Systems Security Management</p> <p>General comment:</p> <p>This section should be broken into two sections. One section should discuss security management at the Control Center and Power Plant (attended) and the Substation (unattended). While there are generic commonalities between the two Cyber environmental, the technical, logistic, personnel, and access differences are sufficient to warrant different management solutions. In addition, the Substation Cyber environment is much more restricted by legacy systems technical limitations than Control Centers and Power Plants.</p> <p>This section is too prescriptive when specifying measurements as in the case of "Retention of System Logs". The specifics of "how" an entity complies with a requirement should be left to the entity to determine and defend. There should be more use of the term "or other mitigating controls" throughout this section in order the address the reality that critical Cyber systems that are less than three years old may have components that exhibit legacy type restrictions when dealing with Patch Management for example.</p> <p>In lieu of restructuring this section, the following specific comments are necessary.</p> <p>Specific Comments:</p> <p>Page 26, Introduction</p> <p>Insert after first sentence....."Many of the requirements in this section will not be applicable in the critical Substation environment since they are typically unmanned and the legacy technology is much more restrictive. Each entity will have to modify or adjust the requirements below to deal with environmental, technical, logistic, personnel, and access differences between attended facilities such as Control Centers and Power Plants and critical Substations which are typically unattended."</p> <p>Page 26, (a)(1) Requirements -- Test procedures</p> <p>Insert at the end of second sentence...."or other mitigating controls"</p> <p>Page 26, (a)(2) Account and Password management:</p> <p>Insert into the first sentence after "establish"... "a system and user"</p> <p>Replace the last sentence with...."The responsible entity must establish and implement password management practices, review systems, and documentation that includes but is not limited to :"</p> <p>Page 26, (a)(2)(i) Strong Passwords:</p>	<p>1306 The standard will be enhanced to differentiate between attended and unattended locations.</p> <p>1306.a.01 The drafting team believes that mitigating controls are not a possible.</p> <p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02.i The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02.ii The drafting team believes individual accounts should be utilized where technically possible.</p> <p>1306.a.02.iv This intent of the standard is that sufficient audit material is present to provide accountability to support the investigation of an event in addition to supporting a compliance audit.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The drafting team is in agreement with your comments and will revise the draft accordingly.</p> <p>1306.a.05 The drafting team agrees with your comment and has updated the standard to address unattended facilities. The drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should</p>

Name	Company	Comments	Responses
		<p>Replace the paragraph with..."Passwords shall be changed periodically using a combination of alpha, numeric, and special characters wherever possible, to reduce the risk of password cracking."</p> <p>Page 26, (a)(2)(ii) Generic Account Management: Replace the last two sentences with..."Where technically and operationally feasible, individual accounts must be used, as opposed to group accounts. Where individual accounts are not feasible, other mitigating controls must be put in place and documented."</p> <p>Page 27, (a)(2)(iv) Acceptable Use Replace the last sentence with..."The policy must support a compliance audit of all account usage."</p> <p>Page 27, (a)(3) Security Patch Management Replace the last sentence with..."In the event that immediate installation is not possible, other mitigating controls must be implemented."</p> <p>Page 27, (a)(4) Integrity Software Replace sentence with.... "A formally documented process governing the application of anti-malware system integrity tools must be employed to prevent, limit, and/or mitigate their introduction or exposure to critical Cyber assets at and within the electronic security perimeter."</p> <p>Page 27, (a)(5) Identification of Vulnerabilities and Responses Replace the first sentence with..."Where technically and operationally feasible, an industry standard vulnerability assessment or scan shall be performed periodically that includes a diagnostic review of the access points, open ports/services, modems, default accounts, and patch management."</p> <p>Page 27, (a)(6) Retention of System Logs Replace the paragraph with..."Where technically and operationally feasible, all critical Cyber assets must generate logs/reports of related system events. The responsible Entity must retain these logs/reports for a reasonable period of time as necessary for a compliance audit and incident response purposes."</p> <p>Page 27, (a)(7) Change Control and Configuration Management Replace the paragraph with..."The responsible Entity shall establish a Change Control Process for modifying hardware and software for critical Cyber assets. The process should include change management procedures for testing, modification, compliance auditing, failure management, and overall integration integrity, where technically and operationally feasible."</p> <p>Page 28, (a)(8) Disabling Unused network Ports/Services Delete this element...Redundant. Covered in (a)(5)</p>	<p>most appropriately perform the test.</p> <p>1306.a.06 The following rewording will be discussed with the drafting team for possible use in 1300 draft 2: "Using manual procedures or monitoring systems either internal and/or external to critical cyber assets, it must be possible to create an audit trail from logs of security-related events affecting the critical cyber assets. The responsible entity must determine and document its own logging strategy to fulfill the requirement, and shall retain said log data for a period of ninety (90) days. In the event a cyber security incident is detected within the 90-day retention period, the logs must be preserved in an exportable format for a period of three (3) years, for possible use in further event analysis."</p> <p>1306.a.07 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.08 Not necessarily... Identifying available ports/services either pre- or post-hardening is not the same as actually disabling ports – one is 'monitor', the other 'defend'...</p> <p>1306.a.09 This could indeed be true. The drafting team may have been trying to make a point of emphasis about securing dial-up communications. This will be raised for discussion by the drafting team for inclusion/deletion in 1300 draft 2.</p> <p>1306.a.10 The intent/spirit of "technically feasible" is certainly appreciated, but what about "financially feasible?" In both cases 'feasible' can only be understood "relative to what?" The word just creates more questions. In the end, each responsible entity will have to create the required capability using logic it feels is defensible as to its reasonableness.</p> <p>The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented"</p>

Name	Company	Comments	Responses
		<p>Page 28, (a)(9) Dial-up Modems</p> <p>Delete this element...Redundant. Covered in (a)(5)</p> <p>Page 28, (a)(10) Operating Status Monitoring Tools</p> <p>Insert before the word "Computer"... "Where technically feasible, ..."</p> <p>Page 28, (a)(11) Back-up and Recovery</p> <p>Replace the first sentence with.... "Information and data that is resident or required by computer systems used to manage critical electric infrastructure must be backed-up on a regular basis, where technically feasible. The back-up must be stored in a remote or hardened site some distance away from the critical Cyber assets."</p> <p>Pages 28 -31, (b) -- (f)</p> <p>CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.</p>	<p>1306.a.11 The wording suggested will be discussed by the drafting team in preparation of 1300 draft 2. The requirement to periodically test the viability of media used to store information for a long period will in all likelihood remain.</p>

Name	Company	Comments	Responses
Tom Pruitt	Duke Energy	<p>Consider deleting references for backup and recovery (section 11) from 1306 and move as applicable to 1308 "Recovery Plans"</p> <p>1306(2), pg 28 It is expensive and time consuming to audit all accounts quarterly. Suggest this be at most annually.</p> <p>1306(5), pg 27 Annual reviews of this nature are expensive and can be dangerous if improperly done in a real-time operation environment, in fact potentially impacting the critical cyber systems themselves. Duke does not agree with this requirement.</p> <p>1306(6), pg 27 Retaining all system logs for 90 days is problematic do to the significant sizes. Large amounts of storage media and/or operational costs are required. Suggest a 30 day requirement for retaining these logs.</p> <p>1306(a)(1) In many cases, there is no "controlled, non-production environment" available for existing, sometimes "legacy," equipment.</p> <p>1306(a)(2) &amp; (i)</p> <p>Many "legacy" systems are not capable of modern "strong" passwords, etc. The definition of strong passwords is different between this draft and the FAQ document. The definition of strong passwords needs to be clarified.</p> <p>1306(a)(2)(ii) Management of individual passwords for a particular application is quite burdensome for a system with potentially thousands of users. Legacy systems do not necessarily incorporate domain type technology. In these cases, passwords have to be managed for each individual system. Thus, some power plants use generic passwords for some less critical applications. Does this apply to all Operating Systems?</p> <p>1306(a)(5) If the network is properly isolated (logical and/or physical), this type vulnerability assessment lends little value in an "annual" frequency.</p> <p>1306(a)(8) Legacy systems or vendor developed systems cannot support this without voiding the warranty in some cases.</p> <p>1306(10), pg 28</p> <p>Many SCADA systems do not have or are not going to support operating status tools. Also, in many cases bandwidth is not going to support the added network traffic and actually critical SCADA traffic may be delayed. Duke does not agree with this requirement in its current form. This is a very large burden for a stand alone system. In some cases, the notification is only a status alarm in the control room of a power plant. In some cases, introducing a monitoring function to a particular system increases its vulnerability -- particularly to stand alone systems.</p> <p>1306(a)(10) Regarding "on a regular basis" -- a "backup" of real time data (i.e. tape backup) is virtually useless in a power plant.</p>	<p>1306.a.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>1306.a.02 The drafting team feels it is important to review accounts as least quarterly.</p> <p>1306.a.02 The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception. The drafting team will review the standard and FAQ document for consistency.</p> <p>1306.a.02.ii The drafting team feels the standard should apply to all systems. Where group accounts are required for system operation, a documented policy must exist for managing access to the group account.</p> <p>1306.a.05 The drafting team agrees with your comment and has updated the standard to address unattended facilities. The drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should most appropriately perform the test.</p> <p>1306.a.05 The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application or frequent upgrades are not practical, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.06 Not "everything" needs to be monitored and/or logged. What's truly needed is completely situation-dependent, so the responsible entity will have to create valid audit trails for itself by close examination of processes and procedures in operation. 'Events' are distinguished as being more fundamental than 'incidents'; in fact, the latter is often</p>

Name	Company	Comments	Responses
		<p>There are a wide variety of data historian tools that are much more suited to analyzing transients, etc. Backups should only be performed prior to and after a change is made to the system -- to ensure that you can return to the original state if a problem is encountered in implementing the change.</p> <p>Is a full system restore required for the test?</p> <p>1306(a)(10) &amp; (11)</p> <p>What do these requirements mean?</p> <p>1306(b)(1) In some cases, non-production equipment is not available. "Potential security vulnerabilities"... this is very open-ended leaves a lot to local interpretation. Please clarify.</p> <p>In some cases, non-production equipment is not available.</p> <p>1306(b)(2) Timelines are inconsistent with other requirements in the document -- in this case, 5 working days and 24 hours. A quarterly audit is too often. Suggest the audit be completed at most annually. The time to complete access review for normal movement of personnel should be 10 business days. Suggested wording: "The responsible entity shall maintain a documented password policy and record of annual audit of this policy against all accounts on critical cyber assets. The documentation shall verify that all accounts comply with the password policy and that obsolete accounts are promptly disabled. Upon normal movement of personnel out of the organization, management must review access permissions within 10 working days.</p> <p>For terminations for cause, management (or designee) must review access permissions within no more than 24 hours."</p> <p>Again, legacy systems do not support password interrogation.</p> <p>1306(b)(3) A monthly review of all vendor security patches and Operating system upgrades is too frequent.</p> <p>"vender" should be spelled "vendor."</p> <p>1306(b)(4) Many patches require a reboot of equipment to take effect. This cannot be done on a monthly basis if the equipment is in service. Does this apply to all Operating Systems?</p> <p>1306(b)(8) &amp; (9) Please define what is meant by "regular audit."</p>	<p>composed of one or more of the former. Examples of events are system administrator execution of privileged commands, both successful and unsuccessful, extended failed login attempts, new account creation, configuration changes, and discovery of network port-probing, to name but a few. At the application level, examples could be logs of system re-directs, or logging of attempts to manually modify production data... It is felt that a 30 day retention window is too short for purposes of identifying low-frequency vulnerability probing conducted over a long period of time.</p> <p>1306.a.08 Suggest discussion and modification of vendor agreements to allow disabling of what are known to be unused ports/services. If they are used by an application, then they aren't unused.</p> <p>1306.a.10 The following wording will be discussed by the drafting team for potential use in 1300 draft 2: "For maintaining situational awareness, critical cyber assets used for operating critical infrastructure must include or be augmented with automated and/or process tools, where possible, to monitor operating state, utilization and performance, and cyber security events experienced by the critical cyber assets themselves, and issue alarms for specified indications, as implemented</p> <p>"</p> <p>1306.a.10 What to back-up and when to back it up is best determined by the responsible entity. The intent of this requirement is: 1) back-up what you need to in order to recover from any of a range of contingencies; 2) Move a copy far enough away so the same disaster that got the data center doesn't get the back-ups; 3) if the back-up is stored for a prolonged period, test the media periodically to be sure it is still readable should it be necessary to do so. The accepted practice is to conduct random media tests of just a small percentage of the total, selected across the span of the back-up volume. The intent is to determine if the media is failing, so that if the data is important it can be moved to another store as appropriate.</p> <p>1306.a.10 1306.a.10 - Inadequate "situational awareness" was a finding from the investigation of the NE blackout of 2003, and this requirement is about situational awareness of networked-computing infrastructure deemed to be critical cyber assets, particularly host computers and high-speed data communications lines. Salient things to monitor can include</p>

Name	Company	Comments	Responses
			<p>CPU utilization, memory utilization, running processes, disk partition usage, hung daemons, defunct process queues, line/network throughput, denial of service attacks, and so on...</p> <p>Each responsible entity will define, implement, and document what it needs to monitor in order to establish and maintain situational awareness of its set of critical cyber assets in operation. The permuted combinations of automated and process tools that might be employed are many and situation-dependent.</p> <p>1306.a.11 - 1) back-up what you need to in order to recover from any of a range of contingencies; 2) Move a copy far enough away so the same disaster that got the data center doesn't get the back-ups; 3) test the media periodically to be sure it is still readable should it be necessary to do so.</p> <p>1306.a.11 The two sections noted talk about different things. 1308 is about disaster recovery and business continuity planning. The backups created as per section 1306, among other things, are used as part of the recovery processes defined in 1308.</p> <p>1306.b.01 The drafting team believes a controlled non-production environment is necessary to avoid disruption to production systems and operations as a result of testing activities. The drafting team feels the standard should apply where technologically feasible. If there are systems where this is not possible, then compensating measures should be taken and documented or it should be documented as a business case exception.</p> <p>The drafting team will update the standard to state known vulnerabilities instead of potential.</p> <p>1306.b.02 A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes."</p> <p>1306.b.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System</p>

Name	Company	Comments	Responses
			<p>Patch may break the application or frequent upgrades are not practical, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.b.04 The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application or frequent upgrades are not practical, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.b.08 The word “annual” will replace the word “regular” in 1306.b.09 draft 2</p>

Name	Company	Comments	Responses
William Smith	Allegheny Energy	<p>1306 Systems Security Management</p> <p>Generally, this section is onerous and does not account for the many differences in electronic systems. Rewriting the section as recommended by the EEI Security Committee would provide the flexibility for the various legacy systems that do not lend themselves for many of the mandated controls.</p> <p>Specific concerns include:</p> <p>1306(a)(1) - Test procedures should also apply to devices that manage the Critical Cyber Asset Electronic perimeter (firewalls).</p> <p>1306(b)(4) - The last sentence is a fragment and confusing.</p> <p>1306(b)(10) - Remove the "a" between maintain and documentation</p> <p>1306(e)(3)(iii)(B)(3) - Quarterly Audits -- Where are the quarterly audits mandated?</p> <p>1306(a)(2)(ii) - Where generic accounts (a single account used by many people) are used, the "scope" (type and locations of access, user rights of these accounts) of these accounts should be as small as possible to minimize the potential access "footprint". Where generic accounts are used outside the electronic security perimeter to access data from a Critical Cyber Asset, only limited read only access should be allowed. Revise the standard to allow these types of generic accounts.</p> <p>1306(a)(3) - Installations of patches on control system computers may require a plant outage before this can be done without potentially disrupting plant operation. The word "timely" in this section infers that the patches are to be installed as soon as possible. Revise the standard to be clearer that the patches are to be installed as directed by formal security patch management practice.</p> <p>Also, does this apply to all levels of patches for all operating systems and applications?</p> <p>1306(a)(4) - Some real-time software does not work correctly along with virus software. In such cases, manufactures of such software should be encouraged to document incompatibilities. Revise to standard to allow for this exclusion.</p>	<p>1306 The standard will be enhanced to differentiate between attended and unattended locations.</p> <p>1306.a.01 Agreed. The standard applies to all critical assets as determined by the entity's risk assessment.</p> <p>1306.a.02.ii The responsible entity should determine it's own generic account management strategy that fits the requirement. This strategy must be sufficient to provide accountability to support the investigation of an event.</p> <p>1306.a.03 The draft will be updated to reflect an associated risk assessment to determine timely installation of patches.</p> <p>The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.04 The intended interpretation of the standard is that on systems where updates are not possible, e.g., the Operating System Patch may break the application or frequent upgrades are not practical, an alternate method of protection must be put in place. Examples are: a security appliance in place, or containing network connection within a local area network that is not connected back to the corporate network or Internet. See FAQs on Security Patch Management and Anti-Virus Software.</p> <p>1306.a.05 The drafting team agrees with your comment and has updated the standard to address unattended facilities. The drafting team specified a controlled test because of the risks involved. The drafting team is only specifying that the test be performed. The responsible entity can determine who should most appropriately perform the test.</p> <p>1306.a.07 Security related system events should be determined by the entity based on their environment. The entity should determine its own logging strategy that fits the requirements. The strategy should be sufficient to support the investigation of an event and that the integrity of these electronic records is maintained.</p>



Name	Company	Comments	Responses
		1306(a)(5) - Hiring a 3rd party to do intrusion testing can be vulnerability in itself. Revise the standard to exclude penetration testing as a diagnostic review.	1306.a.11 The standard for Defense Department systems run in bunkers is to store back-up copies at a different site. Unless power stations are immune to tornados and hurricanes the requirement to store back-ups off-site shall remain.
		1306(a)(7) - Can more detail be provided on what is meant by audit trails for all security related system events?	
		1306(a)(11) - For Power Stations, it should be sufficient to store backups onsite in a safe location. (A safe location would be a secure location, protected from fire, explosion, electromagnetic, and chemical hazards.). Revise the standard to indicate this.	1306.b.02 1) The drafting team agrees with your comment and will revise the draft accordingly. A review of the standard will be conducted for consistency between sections. The standard will be revised to state "24 hours for cause, or seven calendar days for other changes." 2) The intent is that appropriate action will be taken upon completion of the review.
		1306(b)(2): 1. In this and other places, access permissions are to be reviewed and revised within 24 hours. Recommend that only "for cause" terminations adhere to the 24-hour time frame. Normal access permission revisions due to retirement, transfer, etc. should be completed within five business days.	1306.b.04 The drafting team is in agreement with your comments and will revise the draft accordingly.  1306.b.10 Thank you
		2. Is the review within 5 days meant to also include action taken in 5 days?	1306.e.03.iii.B.3 The compliance measures will be reviewed and revised accordingly.

# Section 1307 Comments and Drafting Team Response

Name	Company	Comments	Drafting Team Responses
A. Ralph Rufrano	NYPA	<p>1307, spell out and provide clarification on the acronyms throughout.</p> <p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."	
		to	
		"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."	
		Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents for three calendar years."	
		Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."	
		1307.d.1 there is a 90 day reference that does not appear in the measures.	

Name	Company	Comments	Drafting Team Responses
Allen Berman	LIPA	<p>1307 Incident Response Planning</p> <p>Comment: Would an EMS going down due to hardware/software problems and not necessarily a cyber security issue be considered a reportable incident?</p>	<p>No, the section has been updated to reflect that Cyber Security Incidents must be reported. The definitions have also been updated to specifically define Cyber Security Incident.</p>

Name	Company	Comments	Drafting Team Responses
Charles Yeung	SPP	<p>1307 Incident Response Planning: Bullet resequencing needs to be consistent. Numbering of sub bullets in (b) Measures picks up where (a) Requirements left off. Sections following (b) Measures start with repeated (b).</p> <p>1307 (b) (6)\ Measures: ". . . records of incidents and cyber security incidents. . ." needs to be reworded. Does the first "incidents" refer to physical incidents?</p>	<p>Will be correct draft v2</p> <p>The paragraph has been updated, the refrence to "incident" has been removed, however "Cyber Security Insident" would still include phisical security insidents related to critical cyber assets.</p>

Name	Company	Comments	Drafting Team Responses
Charlie Salamone	NSTAR	<p>1307 - Change title of requirement to "Incident Reporting and Response Plan"</p> <p>1307.a.2 - Requirement should be applicable to malicious and or suspicious security incidents; need to clarify.</p>	<p>Title has been changed to "Insident Reporting and Response Planning"</p> <p>The section has been updated to reflect that Cyber Securitiy Incidents must be reported. The definitions have also been updaed to specifically define Cyber Security Incident.</p>

Name	Company	Comments	Drafting Team Responses
Chris DeGraffenried	NYPA	<p>1307, spell out and provide clarification on the acronyms throughout.</p> <p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p>	<p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4. This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>"Incident and Cyber Security Incident Reporting" has been chnaged to "Cyber Security Insident Reporting"</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the refrence to "incident" has been removed and now only references Cyber Security Insident.</p> <p>Change 1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1 The paraprph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."</p> <p>Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents for three calendar years."</p> <p>Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p>	



Name	Company	Comments	Drafting Team Responses
Dave Norton	Entergy Transmission	51. Page 33 - (d) Levels of Non-Compliance (3) Level Three (ii) "There have been no documented cyber security incidents reported to the ESISAC." If there were no incidents to report, why would this be a Level 3 noncompliance? This probably needs to be reworded to indicate that there were incidents but they were not reported.	(d)(3)(ii) This paragraph has been updated to clarify.

Name	Company	Comments	Drafting Team Responses
David Kiguel	Hydro One	<p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from "Incident and Cyber Security Incident Reporting" to "Security Incident Reporting". Change from "The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)." to "The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident".</p> <p>In 1307, spell out and provide clarification on the acronyms throughout.</p> <p>-----</p> <p>In 1307.d.1 there is a 90 day reference that does not appear in the measures.</p> <p>-----</p> <p>--</p> <p>In the beginning of 1307, change</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>-----</p> <p>Change 1307.b.5 from</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p> <p>to</p> <p>"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."</p>	<p>1307.a.4: This requirement was included in 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>1307:Acronyms have been defined.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requirements as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p>

Name	Company	Comments	Drafting Team Responses
		<p>----- -----</p> <p>Change 1307.b.6</p> <p>"The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents for three calendar years."</p> <p>----- ---</p> <p>Change 1307.b.7</p> <p>"The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."</p>	

Name	Company	Comments	Drafting Team Responses
David Little	Nova Scotia Power	<p>1307 1307, spell out and provide clarification on the acronyms throughout.</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p> <p>Change 1307, from; Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified. to Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified.</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from; Incident and Cyber Security Incident Reporting to Security Incident Reporting.</p> <p>and also Change from; The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP). to The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP).</p> <p>Refer to our definition of a security incident .</p> <p>Change 1307.b.5 from; The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements. to The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements.</p> <p>Change 1307.b.6 from The responsible entity shall retain records</p>	<p>1307:Acronyms have been defined.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requirements as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p>

Name	Company	Comments	Drafting Team Responses
		<p>of incidents and cyber security incidents for three calendar years to</p> <p>The responsible entity shall retain records of security incidents for three calendar years</p> <p>Change 1307.b.7 from The responsible entity shall retain records of incidents reported to ESISAC for three calendar years. to</p> <p>The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years</p>	

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	<p>1307</p> <p>(1) The responsible entity shall develop and document an incident response plan. The plan shall provide and support a capability for reporting and responding to physical and cyber security incidents to eliminate and/or minimize impacts to the</p> <p>- Physical incident response, if confined to the cyber assets, is within scope of this policy. Each entity probably has a physical security incident reporting and response process that addressed site access, vandalism, theft, and other activities. This may be distinctly different than the cyber security incident response process and may be covered by other policy. Wording changes may clarify the boundaries between these two processes and not be mistaken to indicate that an integrated plan is necessary.</p> <p>(3) Electronic and Physical Incident Response Actions: The responsible entity shall define incident response actions, including roles and responsibilities of incident response teams, incident handling procedures, escalation and communication plans. The plans shall include communication with partner entities, as appropriate - These actions can be documented in the MOUs/MOAs suggested earlier.</p>	<p>(1) The reference to "physical" has been removed. The intention of this standard is that only physical incidents that are related to cyber assets are covered. Those are included in "Cyber Security Incidents"</p> <p>(3) The drafting team concluded that this detail level of specification is not appropriate in the standard.</p>

Name	Company	Comments	Drafting Team Responses
Ed Stein	FirstEnergy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34: 1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents. Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p>	<p>Definitions have been added for Cyber Security Incident, and reference the "Incident" removed. Only Cyber Security Incidents are now referenced in the section.</p> <p>The reference to reportable incident has been removed</p> <p>Detail procedures will need to be defined by each responsible entity, the requirement in the standard is that information related to Cyber Security Incidents" is retained for 3 years.</p>

Name	Company	Comments	Drafting Team Responses
Francis Flynn	National Grid	<p>1307, spell out and provide clarification on the acronyms throughout the document.</p> <p>1307 Incident Response Planning General Comment – Change all ‘Incident’ to ‘Security Incident’</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p> <p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard.</p> <p>Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p>	<p>1307:Acronyms have been defined.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requirements as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>



Name	Company	Comments	Drafting Team Responses
		<p>Refer to our definition of a "security incident" as mentioned earlier in this comment form.</p> <p>Change 1307.a.4 from: Incident and Cyber Security Incident Reporting: The responsible entity shall report all incidents and cyber security incidents</p> <p>to:</p> <p>Cyber Security Incident Reporting: The responsible entity shall report all cyber security incidents...</p> <p>Change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p> <p>to</p> <p>"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."</p> <p>Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."</p> <p>to</p> <p>The responsible entity shall retain summary documents of cyber security incidents for three calendar years. Specific logs of cyber security incidents used must be preserved for a period one (1) year.</p> <p>Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain security incident documents submitted to ESISAC for three calendar years."</p> <p>Change 1307.c.2 from:</p> <p>The responsible entity shall keep all records related to incidents</p>	

Name	Company	Comments	Drafting Team Responses
		<p>and cyber security incidents for three calendar years. This includes, but is not limited to the following:</p> <ul style="list-style-type: none"> <li>(i) System and application log file entries related to the incident,</li> <li>(ii) Video, and/or physical access records related to the incident,</li> <li>(iii) Documented records of investigations and analysis performed,</li> <li>(iv) Records of any action taken including any recovery actions initiated.</li> <li>(v) Records of all reportable incidents and subsequent reports submitted to the ES-ISAC.</li> </ul> <p>to:</p> <p>The responsible entity shall preserve logs related to security incidents for one (1) calendar year in accordance with 1306.a.6. All other documents related to cyber security incidents shall be kept for three calendar years. This includes, but is not limited to the following:</p> <ul style="list-style-type: none"> <li>(i) Video, and/or physical access records related to the incident,</li> <li>(ii) Documented records of investigations and analysis performed,</li> <li>(iii) Records of any action taken including any recovery actions initiated.</li> <li>(iv) Records of all reportable incidents and subsequent reports submitted to the ES-ISAC.</li> </ul> <p>Change 1307.d.3.ii from:</p> <p>There have been no documented cyber security incidents reported to the ESISAC.</p> <p>To:</p> <p>There are documented cyber security incidents that meet the reporting threshold of the ESISAC Indications, Analysis &amp; Warning Program (IAW) Standard Operating Procedure (SOP)that have not been reported.</p>	

Name	Company	Comments	Drafting Team Responses
Francois Lemay	Brascan Power	Eliminate or significantly reduce the scope of the section "1307.a.4 The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis & Warning Program (IAW) Standard Operating Procedure (SOP)." As written, the reporting could be extremely onerous and inconsequential	The section has been updated , the references to "incident" have been removed. The definitions have also been updated to specifically define Cyber Security Incident. This should clarify that reporting is only required for security incidents.

Name	Company	Comments	Drafting Team Responses
Gary Campbell		<p>1307</p> <p>Requirements</p> <p>1 This requirement should also provide language to maintain the described incident response plan.</p> <p>4 What does "all incidents " mean? If it is not Cyber related then should it be included here?</p> <p>Measures</p> <p>5 I suggest the wording be changed to read " The responsible entity shall have and maintain documentation ....." This will then follow the requirements.</p> <p>6 I do not believe the requirements stated that entities shall retain records so then how can we measure them on this item? Maybe we should look at ensuring the procedures are in place? This could then become part of the Compliance Monitoring Process section?</p> <p>7 This statement could be reworded to say " the responsible entity shall have evidence of reporting incidents to the ESISAC ....." . The statement as written should then be moved to the Compliance Monitoring Process section.</p> <p>Compliance Monitoring Process</p> <p>2 (i,ii,iii,iv,v) Should these be included under the requirements section as you are defining what should be included as part of the documentation and therefore somewhere this should be identified in a procedure?</p> <p>Levels of Noncompliance</p> <p>1 What are known changes? How is the CM to know if he has a these known changes? If the documented is to be updated periodically is should specified in the requirements and then measured. It can then be reviewed for updates and accessed accordingly.</p> <p>2 (i) It was not required to update or review the incident response plan. Nor do we really have measure for this item.</p>	<p>Requirments:</p> <p>1. Maintenace of the plan is covered in the "Measures" section.</p> <p>4. "all incidents" has been changed to " all cyber security incidents"</p> <p>Measures:</p> <p>5. Drafting team respectfully disagrees.</p> <p>6. The measures are inended to be those measures (procedure/processes) to be implemented by responsible entities that support the requirements.</p> <p>7.Drafting team respectfully disagrees.</p> <p>Compliance Monitoring Processes:</p> <p>2. Drafting team respectfully disagrees.</p> <p>Levels of Non compliance:</p> <p>1. Any change that should be reflected in documnetation.</p> <p>2.i. This is addressed in Levels of non compliance</p> <p>2.ii.The detail procedures to be followed by each responsible entity are to be defined by that entity.</p> <p>3.i. E.g. Not aproved, not finalized etc.</p>

Name	Company	Comments	Drafting Team Responses
		<p>(ii) I think we go past what has been required and measured. I can not find what the records should contain in this document or what records specifically. Isn't this standard to ensure cyber security? We should leave the record keeping for ESIAC to that group.</p>	
		<p>3 (i) Be mor specific as to what incomplete means?</p>	
		<p>(ii) As read this statement could leave an entity level 4 noncompliant if in all actuality there were no incidences to report to ESIAC. It sort of makes the statement that there must be an incident.</p>	
		<p>4 Does this statement mean there was no plan, no records etc? And to be level 4, does the entity have to have every document missing?</p>	

Name	Company	Comments	Drafting Team Responses
Guy Zito	NPCC	<p>1307, spell out and provide clarification on the acronyms throughout.</p> <p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requirements as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."</p> <p>Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents for three calendar years."</p> <p>Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p>	

Name	Company	Comments	Drafting Team Responses
Howard Ruff	WE Energies	<p>Standard 1307, Sect. a4. Based the definition of an Incident, we would need to report all activities that disrupt functional operation of a cyber asset. This could include such operational items like server reboot after applying a patch. The ISAC would be flooded with these "incident" reports. Reporting should be limited to only security incidents. Strongly recommend that reporting only be required for incidents with malicious intent or of suspicious nature, whether physical or cyber. As written, the section requires reporting of incidents which may result from an equipment failure or software configuration error which have no genesis in an act against the entity. These are likely to be more numerous than actual attacks creating a reporting burden as well as yielding no value to the entity. Non-security related events should be outside the scope of the standard, in any case. Re-edit the section to embrace the amended definition of "security incident" above. The CIPC may have to amend the IAW SOP to recognize its reference by the 1300 standard to ensure harmony between these two documents.</p>	<p>The section has been updated , the refrences to "incident" have been removed. The definitions have also been updtaed to specifically define Cyber Security Incident. This should clarify that reporting is only required for security incidents.</p>



Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34: 1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents. Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>Definitions have been added for Cyber Security Incident, and reference the "Incident" removed. Only Cyber Security Incidents are now referenced in the section.</p> <p>The reference to reportable incident has been removed</p> <p>Detail procedures will need to be defined by each responsible entity, the requirement in the standard is that information related to Cyber Security Incidents" is retained for 3 years.</p>

Name	Company	Comments	Drafting Team Responses
		<p>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</p> <p>2. ABC does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</p> <p>ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
John Blazeovitch	Exelon	<p>1307.b.6 Records should be retained for cyber security incidents only. We recommend that the sentence read: The responsible entity shall retain all records related to cyber security incidents for three calendar years.</p> <p>1307.c.2 Records should be retained for cyber security incidents only. We recommend that the sentence read: The responsible entity shall retain all records related to cyber security incidents for three calendar years.</p>	<p>1307.b.6 and 1307.c.2: The paragraphs have been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p>

Name	Company	Comments	Drafting Team Responses
John Hobbick	Consumers Energy	<p>1307 – Incident Response Planning</p> <p>4) This section is written to include both physical and cyber security incidents. This standard should focus on cyber incidents. Any physical incident that impacts cyber assets should be reported as a cyber incident, other physical incidents should be addressed in other standards</p>	The section has been updated to clarify.

Name	Company	Comments	Drafting Team Responses
Karl Tammer	ISO-RTO Council	Some of the reviewers were not clear on what ESISAC meant. Should be spelled out.	ES ISAC has been defined in the section, in addition there is a section in the published FAQ that deals with the ES ISAC.

Name	Company	Comments	Drafting Team Responses
Kathleen Goodman	ISO-NE	<p>1307 Preamble ... must be monitored on a continuous basis - different terminology - previously used 24 hours a day, 7 days a week Need to clarify and be consistent through standard. Remove “or cyber security incidents” from last sentence.</p> <p>1307 Requirements Rewrite/remove a few words in this section to clarify: “(1) The responsible entity shall develop and document an incident response plan. The plan shall provide and support a capability for reporting and responding to physical and cyber incidents to eliminate and/or minimize impacts to the organization. The incident response plan must address the following items: (2) Incident Classification: The responsible entity shall define procedures to characterize and classify events (both electronic and physical) as either incidents or cyber security incidents. (3) Incident Response Actions: The responsible entity shall define incident response actions, including roles and responsibilities of incident response teams, incident handling procedures, escalation and communication plans. (4) Security Incident Reporting: The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning Program (IAW) Standard Operating Procedure (SOP).” (4) What is the IAW SOP? Needs more explanation. If it is some other standard, NERC standard process does not allow cross referencing.</p> <p>1307 Measures (6) Rewrite as “The responsible entity shall retain records of incidents for three calendar years.” (7) Rewrite as: “The responsible entity shall retain records of security incidents reported to ES-ISAC for three calendar years.” (7) ESISAC - Who is this, spell it out - also abbreviation is not used consistently. Is it ESISAC or ES-ISAC?</p> <p>1307 Compliance Monitoring (2) Remove words " ... and cyber security ... " (2.v) Replace “reportable” with “security”</p>	<p>1307:The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>Requirements 1: The paragraph has been updated to clarify and be consitent with the section.</p> <p>2: The parapraph has been updated to clarify and be consitent with the section.</p> <p>3:The drafting team concluded that no changes were required.</p> <p>4: ES ISAC has been defined in the section, in addition there is a section in the published FAQ that deals with the ES ISAC.</p> <p>Measures 6 The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>7 This paragraph has been combined with b.6. The section has been to refrence ES ISAC throughtout.</p> <p>Compliance Monitoring: 2. The paragraph has been updated to reflct the other changes in the section, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>2.v "reportable insident " has been replaced with "cyber security incident" consistent with the rest of the section.</p>

Name	Company	Comments	Drafting Team Responses
Ken Goldsmith	Alliant Energy	<p>1307 Incident Response Planning</p> <p>Only security incidents should be reported. Remove any language that differentiates between incident and security incident.</p>	<p>The section has been updated , the references to "incident" have been removed. The definitions have also been updated to specifically define Cyber Security Incident. This should clarify that reporting is only required for security incidents.</p>

Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	<p>Section 1307</p> <p>Retitle this section to be more specific and clear: “Incident Reporting and Response Plan.”</p> <p>(a)(2) – Delete this entire subsection (and revise and renumber format), consistent with the revision in the Definitions to remove reference to “Incident.” The standard should only be applicable to “security” (malicious and/or suspicious) incidents. Equipment and system failures, especially for large companies, are too common and unimportant to necessitate reporting.</p> <p>(a)(4) – The IAW-SOP should be under revision, and this reference should perhaps even be to the CIPIS, rather than the IAW-SOP.</p> <p>(b) – Formatting: revise and renumber.</p> <p>(b)(2)(as revised – “(b)(6)” as drafted), and (c)(2) – As noted above for alarms, the record-keeping requirement is too onerous, especially for large systems, resulting in unnecessarily voluminous files. Records should be kept long-term only regarding “security incidents” Regular files should be “turned over” after one year.</p>	<p>Title has been changed to "Insident Reporting and Response Planning"</p> <p>(a)(2)The section has been updated to reflect that Cyber Securitiy Incidents must be reported. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>(a)(4) - This topic is covered in the FAQ. At this point the drafting team concluded that the refrence to the IAW-SOP is appropriate.</p> <p>(b) Will be addressed in version 2 of the draft.</p> <p>(b)(6) - Has been modified to refrence section 1306 for retention of system logs, and the "incident" refrence has been removed. This should clarify what data would need to be retained,</p>



Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34: 1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. Cinergy seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents. Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>Definitions have been added for Cyber Security Incident, and reference the "Incident" removed. Only Cyber Security Incidents are now referenced in the section.</p> <p>The reference to reportable incident has been removed</p> <p>Detail procedures will need to be defined by each responsible entity, the requirement in the standard is that information related to Cyber Security Incidents" is retained for 3 years.</p>

Name	Company	Comments	Drafting Team Responses
		<ol style="list-style-type: none"> <li>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</li> <li>2. Cinergy does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. Cinergy regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</li> </ol> <p>Cinergy recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
Laurent Webber	WAPA	Section 1307, Incident Response Planning. The meaning of the acronym ESISAC should be stated. It would also be helpful to state how to access ESISAC.	<p>The definition has been added.</p> <p>Access to ES ISAC are in the FAQ.</p>

Name	Company	Comments	Drafting Team Responses
Linda Campbell	FRCC	<p data-bbox="535 175 856 199">1307 Incident Response Planning</p> <p data-bbox="535 232 1178 508">(a) (4) The requirements section indicates that “the responsible entity shall report all incidents to the ESISAC in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures.” The ESISAC program does not require all incidents be reported. Along with the suggested change in the security incident definition (see definitions section), we suggest changing this to “The responsible entity shall report to the ESISAC security incidents meeting the reporting criteria in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures.”</p> <p data-bbox="535 540 1024 565">Numbering is messed up – you have 2 (b) sections.</p> <p data-bbox="535 597 1178 734">(d) (3) (ii) There may well be no cyber incidents reported to ESISAC, if none have occurred.. Suggest changing to “One or more cyber incidents meeting the reporting criteria in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures were not reported to the ESISAC.”</p>	<p data-bbox="1299 175 1866 256">(a)(4): The definition has been modified. The drafting team believes the chaged definition will clarify what is to be reported to the ES ISAC.</p> <p data-bbox="1299 289 1866 337">Numbering will be corrected in draft version 2 of the standard.</p> <p data-bbox="1299 370 1808 394">(d)(3)(ii) This paragraph has been updated to clarify.</p>

Name	Company	Comments	Drafting Team Responses
Linda Nappier	Ameren	1307 (a) (4) Where is ESISAC defined?	Definition has been added to paragraph 1307.a.4

Name	Company	Comments	Drafting Team Responses
Lloyd Linke	WAPA - MAPP	1307 Incident Response Planning. The meaning of the acronym ESISAC should be stated. It would also be helpful to state how to access ESISAC.	<p>The definition has been added.</p> <p>Access to ES ISAC are in the FAQ.</p>

Name	Company	Comments	Drafting Team Responses
Lyman Schaeffer	Pacific Gas & Electric	<p>Section 1307: Security Incident Planning</p> <p>Consistent with our comments on the definitions portion of the standard, one of our biggest concerns is the requirement to report all “incidents” rather than reporting “security incidents” where there is reason to believe there is a malevolent cause. As noted earlier, equipment and system failures are common in a large company, and we feel that requiring the reporting of all incidents is not only burdensome for us but counterproductive from a security management perspective as it will potentially inundate the ISAC with repetitive and ultimately useless data. We believe the standard should require only the reporting of security incidents or those failures that result in severe disruptions.</p> <p>This section also requires that the responsible entity maintain a record of all incidents along with any investigations and analyses performed with documentation maintained for three calendar years. Consistent with our earlier comments, we believe this should be limited rather than apply to all “incidents.” Not only will this reduce the required documentation to a more manageable level, but it will also allow us to focus attention more effectively on the type of incidents that this standard was intended to deal with i.e. serious cyber issues.</p>	<p>The section has been updated , the references to "incident" have been removed. The definitions have also been updated to specifically define Cyber Security Incident. This should clarify that reporting is only required for security incidents.</p> <p>The section has been modified to reference section 1306 for retention of system logs, and the "incident" reference has been removed. This should clarify what data would need to be retained,</p>

Name	Company	Comments	Drafting Team Responses
Michael Anderson	Midwest ISO	Incident Reporting – Could the definition of suspected vs. validated incident be made extremely clear? Why the change in reporting to include the ESISAC?	<p data-bbox="1291 170 1904 230">The detail procedures to be followed by each responsible entity are to be defined by that entity.</p> <p data-bbox="1291 256 1904 341">The ES ISAC requirement was included in the 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p>



Name	Company	Comments	Drafting Team Responses
Paul McClay	Tampa Electric Company	<p data-bbox="535 175 858 199">1307 Incident Response Planning</p> <p data-bbox="535 232 1178 508">(a) (4) The requirements section indicates that “the responsible entity shall report all incidents to the ESISAC in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures.” The ESISAC program does not require all incidents be reported. Along with the suggested change in the security incident definition (see definitions section), we suggest changing this to “The responsible entity shall report to the ESISAC security incidents meeting the reporting criteria in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures.”</p> <p data-bbox="535 540 1022 565">Numbering is messed up – you have 2 (b) sections.</p> <p data-bbox="535 597 1178 734">(d) (3) (ii) There may well be no cyber incidents reported to ESISAC, if none have occurred.. Suggest changing to “One or more cyber incidents meeting the reporting criteria in accordance with the Indications, Analysis and Warning Program (IAW) Standard Operating Procedures were not reported to the ESISAC.”</p>	<p data-bbox="1299 175 1850 256">(a)(4): The definition has been modified. The drafting team believes the chaged definition will clarify what is to be reported to the ES ISAC.</p> <p data-bbox="1299 313 1705 337">Numbering will be corrected in draft ver 2</p> <p data-bbox="1299 370 1806 394">(d)(3)(ii) This paragraph has been updated to clarify.</p>

Name	Company	Comments	Drafting Team Responses
Pete Henderson	IMO	<p>1307 Incident Response Planning (d) Levels of Noncompliance 1307 (d) (1) and 1307 (d) (2) (i) require revision. Neither 1307 (a) nor 1307 (b) specify a requirement to update documentation within 90 days or review documentation annually.</p> <p>In a case where records related to the response to a reportable security incident are incomplete, it is unclear whether 1307 (d) (2) (ii) or 1307 (d) (3) (i) applies.</p> <p>1307 (d) (3) (ii) should be reworded to state that a failure to report a reportable incident to ESISAC is a level 3 non-compliance.</p>	<p>1307.a and b : This was intentional, as not to be over redundant. The measure also specifically calls out the documentation must be maintained.</p> <p>1307.d.2.ii and d.3.i: d.2.ii specifically deals with documents supporting incidents while d.3.i deals with documentation of the response plan.</p> <p>1307.d.3.ii: This paragraph has been updated to clarify</p>

Name	Company	Comments	Drafting Team Responses
Ray A'Brial	CHGE	<p>1307 Retitle this section to be more specific and clear: Incident Reporting and Response Plan.</p> <p>1307, spell out and provide clarification on the acronyms throughout.</p> <p>Change 1307, from;</p> <p>Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified.</p> <p>to</p> <p>Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified.</p> <p>(a)(2) delete this entire subsection, consistent with the revision in the Definitions to remove reference to "Incident." The standard should only be applicable to malicious and/or suspicious (security) incidents.</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>Security Incident Reporting.</p> <p>and also Change from;</p> <p>The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP).</p> <p>to</p> <p>The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)." or perhaps even be to the CIPIS, rather than the IAW-SOP.</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Insident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		<p>Refer to our definition of a security incident, change 1307.b.5 from;</p> <p>The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements.</p> <p>to</p> <p>The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements.</p> <p>Change 1307.b.6 from The responsible entity shall retain records of incidents and cyber security incidents for three calendar years.</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents for three calendar years."</p> <p>Change 1307.b.7 from The responsible entity shall retain records of incidents reported to ESISAC for three calendar years.</p> <p>to</p> <p>The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years.</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p>	

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34: 1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security. “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents. Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>Definitions have been added for Cyber Security Incident, and reference the "Incident" removed. Only Cyber Security Incidents are now referenced in the section.</p> <p>The reference to reportable incident has been removed</p> <p>Detail procedures will need to be defined by each responsible entity, the requirement in the standard is that information related to Cyber Security Incidents" is retained for 3 years.</p>

Name	Company	Comments	Drafting Team Responses
		<p>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</p> <p>2. ABC does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</p> <p>ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
Richard Engelbrecht	Rochester Gas & Electric	<p>1307, spell out and provide clarification on the acronyms throughout.</p> <p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been carried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updated to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requirements as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Incident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		<p>to</p> <p>"The responsible entity shall maintain documentation that defines incident classification security incident reporting requirements."</p> <p>Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents for three calendar years."</p> <p>Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."</p> <p>to</p> <p>"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."</p> <p>1307.d.1 there is a 90 day reference that does not appear in the measures.</p>	



Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p>Section 1307: As written, it appears that this the section requires reporting of all incidents including equipment failures or software configuration errors. If this assessment is correct, would all hung-up or failed modems need to be reported? Should non-security related incidents be outside the scope of this standard? We believe the standard should focus only on security incidents. If not the ESISAC may be inundated with repetitive and ultimately useless information possibly masking the security incidents due to the volume of non-security incidents. Are ESISAC reported events available to the public?</p>	<p>The section has been updated , the refrences to "incident" have been removed. The definitions have also been updtaed to specifically define Cyber Security Incident. This should clarify that reporting is only required for security incidents.</p>

Name	Company	Comments	Drafting Team Responses
Robert Pelligrini	United Illuminating	<p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p> <p>to</p> <p>"The responsible entity shall maintain documentation that defines</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Insident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		incident classification security incident reporting requirements."	
		Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents for three calendar years."	
		Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."	
		1307.d.1 there is a 90 day reference that does not appear in the measures.	

Name	Company	Comments	Drafting Team Responses
Robert Strauss	NYSEG	<p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p> <p>to</p> <p>"The responsible entity shall maintain documentation that defines</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Insident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		incident classification security incident reporting requirements."	
		Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents for three calendar years."	
		Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."	
		1307.d.1 there is a 90 day reference that does not appear in the measures.	

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>1307 (Incident Response Planning)</p> <ul style="list-style-type: none"> <li>• 1307(b)(5)-(7) should be re-sequenced (1)-(3).</li> <li>• 1307(c)(2) No performance reset period stated.</li> <li>• 1307(d)(1)(i) "Documentation exists, but has not been updated with known changes within the 90-day period and/or " No 90-day update period is specified in 1307.</li> <li>• 1307(d)(3)(ii) "There have been no documented cyber security incidents reported to the ESISAC." Maybe there have been no incidents! As worded this is unclear. This should be restated as "Cyber security incidents have occurred but have not been reported to ESISAC".</li> <li>• (1st paragraph) Add to the end of the paragraph – “An incident is defined as an event or incident which is determined to have resulted in an actual or attempted intrusion, disruption, or other compromise to covered cyber or physical assets.”</li> </ul>	<p>Formatting will be corrected in draft ver2</p> <ul style="list-style-type: none"> <li>• 1307(c)(2) No response at this time, under discussion with NERC Compliance</li> <li>• 1307(d)(1)(i) Paragraph has been updated to clarify. However the 90 day period currently is only defined in the Levels section.</li> <li>• 1307(d)(3)(ii) The paragraph has been updated to reflect suggestion</li> <li>• (1st paragraph) Definition of Cyber security Incident has been updated making the definition in the section unnecessary.</li> </ul>

Name	Company	Comments	Drafting Team Responses
S. Kennedy Fell	NYISO	<p>Change 1307, from;</p> <p>"Incident Response Planning defines the procedures that must be followed when incidents or cyber security incidents are identified."</p> <p>to</p> <p>"Incident Response Planning defines the procedures that must be followed when a security incident related to a critical cyber asset is identified."</p> <p>1307.a.4 makes the IAW SOP a standard. Currently, this is a voluntary program. The pieces of the program that should be a standard need to be in this standard. Change from;</p> <p>"Incident and Cyber Security Incident Reporting"</p> <p>to</p> <p>"Security Incident Reporting".</p> <p>and also Change from;</p> <p>"The responsible entity shall report all incidents and cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>to</p> <p>"The responsible entity shall report all security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning (IAW) Program's Standard Operating Procedure (SOP)."</p> <p>Refer to our definition of a "security incident", change 1307.b.5 from;</p> <p>"The responsible entity shall maintain documentation that defines incident classification, electronic and physical incident response actions, and cyber security incident reporting requirements."</p> <p>to</p> <p>"The responsible entity shall maintain documentation that defines</p>	<p>1307:Acronyms have been defined.</p> <p>1307: The section has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.d.1:The paragraph has been modified to clarify the level of non-compliance.</p> <p>1307:The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.a.4: This requirement was included in 1200 series standard and has been caried over, this has also been addressed in the FAQ published with the DRAFT of 1300.</p> <p>and also</p> <p>The paragraph has been updated, the reference to "incident" has been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p> <p>1307.b.5: The measure is defined to meet the requiremnts as set out in section (a) of 1307.</p> <p>1307.b.6:The paragraph has been updated, the reference to "incident" has been removed and now only references Cyber Security Insident.</p> <p>1307.b.7 this paragraph has been combined with b.6.</p> <p>1307.d.1The paragraph has been modified to clarify the level of non-compliance.</p>

Name	Company	Comments	Drafting Team Responses
		incident classification security incident reporting requirements."	
		Change 1307.b.6 from "The responsible entity shall retain records of incidents and cyber security incidents for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents for three calendar years."	
		Change 1307.b.7 from "The responsible entity shall retain records of incidents reported to ESISAC for three calendar years."	
		to	
		"The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years."	
		1307.d.1 there is a 90 day reference that does not appear in the measures.	



Name	Company	Comments	Drafting Team Responses
Terry Doern	BPA	1307.a.1 As a Federal entity, BPA must report to CIAC, who then reports to ESISAC.	The paragraph has been updated to allow for indirect reporting, the responsibility of reporting will still remain with the responsible entity. A section has also been added to the FAQ.

Name	Company	Comments	Drafting Team Responses
Tom Flowers	Centerpoint Energy	<p>Page 32, 1307 Incident Response Planning</p> <p>General comment:</p> <p>This section should focus on security incidents only and avoid discussion of other forms of incidents.</p> <p>Specific Comments:</p> <p>Page 32, Introduction:</p> <p>Replace the paragraph with this..."Security measures designed to protect critical Cyber assets from intrusion, disruption or other forms of compromise must be monitored on a continuous basis and all detected security incidents must be dealt with, when possible, with a preplanned response. Incident Response Planning defines the procedures that must be in place and effectively executed when Cyber security incidents occur."</p> <p>Page 32, (a)(1) Requirements</p> <p>Delete..."(1)" and replace the second sentence with..."The plan shall provide specific procedures that are to be implemented in the event a Cyber security incident occurs in order to assess, mitigate, contain, or prevent negative impacts to any critical Cyber infrastructure."</p> <p>Page 32, (a)(2) Incident Classification</p> <p>Delete this subsection. If this section focuses on Cyber security incidents and the definition of such an incident is provided in the Definition section, as suggested, this subsection is redundant.</p> <p>Page 32, (a)(3) Electronic and Physical Incident Response Actions:</p> <p>Replace title with..."Incident Response Actions"</p> <p>Replace the paragraph with..."(1) The responsible entity shall define the roles and responsibilities of individuals and incident response teams. In addition, procedures, evidence retention, and communication/contact practices must be unambiguous. "</p> <p>Page 32, (a)(4) Incident and Cyber Security Incident Reporting:</p> <p>Replace title with..."Incident Response Reporting"</p> <p>Replace paragraph with..."(2) The responsible entity shall report all security incidents to the ESISAC as appropriate"</p> <p>Pages 32 -33, (b) – (e)</p> <p>CenterPoint Energy will defer comments on these subsections based on the gravity and structural nature of comments on the Introduction and Requirements Subsections.</p>	<p>General: The section has been updated to clarify</p> <p>Introduction: The paragraph has been updated to clarify.</p> <p>(a)(1) The paragraph has been updated to incorporate some of the suggested wording.</p> <p>(a)(2) The paragraph has been retained, not all security events are intended to be Cyber Security Incidents as defined. As such classification is an important requirement.</p> <p>(a)(3) Has been changed to "Cyber Security Incident Response Actions" to agree with the definition. The concept of retention is covered under the measures.</p> <p>(a)(4) Has been changed to "Cyber Security Incident Reporting" to agree with the definition. The paragraph has been updated to clarify.</p>

Name	Company	Comments	Drafting Team Responses
Tom Pruitt	Duke Energy	<p>1307(2), pg 32-33</p> <p>Suggested rewrite:</p> <p>(2) The responsible entity shall keep all records related to cyber security incidents for three calendar years. This includes, but is not limited to the following:</p> <ul style="list-style-type: none"> <li>(i) System and application log file entries related to the security incident,</li> <li>(ii) Video, and/or physical access records related to the security incident,</li> <li>(iii) Documented records of investigations and analysis performed,</li> <li>(iv) Records of any action taken including any recovery actions initiated,</li> <li>(v) Records of all reportable security incidents and subsequent reports submitted to the ES-ISAC.</li> </ul> <p>1307(6), pg 32 Again, this is an example of confusion with the use of the terms “incident” and “security incident”. The term “incident” should not be used in this context. Suggest that this paragraph read: Rewrite to “(6) The responsible entity shall retain records of cyber security incidents for three calendar years.”</p> <p>1307(7), pg 32 Rewrite to “(7) The responsible entity shall retain records of security incidents reported to ESISAC for three calendar years.”</p> <p>1307(b)(5) Should be re-numbered to (b) (1)</p> <p>1307, pg 32 Per the 1300 definitions, this sentence should not include “incidents”, only “security incidents”, which are incidents defined as malicious or suspicious. A large number of incidents could be generated daily, the key is how many are “security incidents”.</p> <p>1307, pg 32 Suggest this sentence read: “The responsible entity shall develop and document a security incident response plan.”</p> <p>1307, pg 32 Suggest this sentence read: “The security incident response plan must address the following items:”</p> <p>1307, pg 32 Again, this is an example of confusion with the use of the terms “incident” and “security incident”. The term “incident” should not be used in this context. The IAW SOP is clear that “incidents” should not be reported. See <a href="http://www.esisac.com/publicdocs/IAW_SOP.pdf">http://www.esisac.com/publicdocs/IAW_SOP.pdf</a>, page 4, section 5, which states:</p> <p>“Reporting is not necessary if it is considered highly probable that the cause is NOT of</p>	<p>This section has been modified.</p> <p>The section has been updated, the references to "incident" have been removed. The definitions have also been updaed to specifically define Cyber Security Incident.</p>

Name	Company	Comments	Drafting Team Responses
		<p>malicious origin, or until such time that a reportable cause is established.” Suggest that this paragraph in 1300 read: “Cyber Security Incident Reporting: The responsible entity shall report all cyber security incidents to the ESISAC in accordance with the Indications, Analysis &amp; Warning Program (IAW) Standard Operating Procedure (SOP).”</p>	

Name	Company	Comments	Drafting Team Responses
Victor Limongelli	Guidance Software, Inc.	<p>In addition to the general statements regarding the need for incident response planning in 1307 (which focus only on "Incident Classification," unspecified "Response Actions," and Reporting), the Standard should detail the technical and procedural requirements for an effective cyber security incident response plan. As written, the Standard would allow each organization to define for itself the appropriate level of incident response actions and incident handling procedures. Unfortunately, this approach lowers the overall grid's reliability. The investigation of, and response to, a cyber security incident involving one or more entities or grids can run aground at the vulnerable organization that does not have an effective incident response capability. Thus, the failure of certain organizations can impact other entities, as well as the overall grid. In short, including within the Standard a baseline level of acceptable incident response capabilities will help ensure the integrity and reliability of the inte</p>	<p>The standard has been created in manner consistent with NERC standards that places the responsibility of detail procedures with the responsible entity.</p>

Name	Company	Comments	Drafting Team Responses
William Smith	Allegheny Energy	<p>1307 Incident Response Planning</p> <p>Allegheny Energy agrees with EEI that the definitions for Incident and Security Incident should be combined to reflect only Security Incidents. (Also refer to Definitions comments above.)</p> <p>1307(d)(3)(ii) – Is there an assumption that all companies will have reportable cyber security incidents? Change wording to “Verified cyber security incidents have not been adequately documented and reported to the ESISAC.”</p>	<p>The definitions have been updated.</p> <p>1307.d.3.ii: This paragraph has been updated to clarify.</p>

# Section 1308 Comments and Drafting Team Responses

Name	Company	Comments	Drafting Team Responses
A. Ralph Rufrano	NYPA	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Allen Berman	LIPA	<p>1308 Recovery Plans 1st paragraph Comment: What is meant by “triggering events” in the following sentence? “Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices”. Suggest that it is not a good practice to “force” operations to relocate to an Alternate Control Center based on time but rather based on the unique circumstances. For instance, sometimes recovery time is pretty much known and it would be best not to relocate strictly because a time limit is reached. Other times, recovery time can not be estimated in which case it most likely is best to relocate after a certain period of time.</p> <p>Comment: Suggest removing the following sentence: There is not requirement for recovery plans for substations and generation plants that have no critical cyber assets.</p> <p>(a) Requirements (2) Comment: Same as comment for 1st paragraph of 1308.document.</p>	<p>1st paragraph moved to the Section 1308 FAQ. a) Requirements (2) has been modified.</p>



Name	Company	Comments	Drafting Team Responses
Chris DeGraffenried	NYPA	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Dave Norton	Entergy Transmission	<p>Page 35 - (e) Levels of Noncompliance (2) reads "Recovery plans have not been reviewed, exercised, or training performed appropriately." This grammar means that a non-compliance will be issued if the training was performed appropriately. To avoid such an error, reword as: "Recovery plans either have not been reviewed, not been exercised, or training has not been performed appropriately."</p> <p>Page 35 - (e) Levels of Noncompliance (3) should be edited to read "Recovery plans address neither the types of events that are necessary nor any specific roles and responsibilities."</p>	<p>Page 35 - (e) Levels of Noncompliance (2) Existing language has been retained</p> <p>Page 35 - (e) Levels of Noncompliance (3) has been modified as suggested.</p>

Name	Company	Comments	Drafting Team Responses
David Kiguel	Hydro One	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
David Little	Nova Scotia Power	<p>1308</p> <p>In 1308, to remain consistent with the scope of Critical Cyber Assets, it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. The requirement for a Backup Control Centre is covered by other NERC Standards. The topic is well outside the scope of this document and does not belong in a Cyber Security Standard.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Deborah Linke	US Bureau of Reclamation	<p>1308 Recovery Plans</p> <p>The entity performing the reliability authority, balancing authority, interchange authority, transmission service provider, transmission operator, generator, or load-serving entity function must establish recovery plans and put in place the physical and cyber assets necessary to put these recovery plans into effect once triggered. Recovery plans must address triggering events of varying duration and severity using established business continuity and disaster recovery techniques and practices.</p> <p>--- Some of the issues discussed in this section relate to continuity of business or continuity of operations. It would appear that these discussions are outside the scope of this standard. It is recommended that this standard only address recovery or contingency plans associated with the cyber asset(s) under consideration. A business or operations continuity plan would identify whether or not the cyber assets require recovery under various general scenarios. That business or operations plan should also address the priority associated with cyber system restoration and the allowable outage and recovery times. Attempting to address business or operations issues within this cyber standard appears out of place and is probably redundant with other NERC guidance or policy.</p> <p>Facilities and infrastructure that are numerous and distributed, such as substations, may not require an individual Recovery Plan and the associated redundant facilities since reengineering and reconstruction may be the generic response to a severe event. Conversely, there is typically one control center per bulk transmission service area and this will require a redundant or backup facility.</p> <p>--- It is unclear whether this is to be read as a requirement for backup control centers. Such centers present considerable investments and bring with them attendant risks (related to attacks mounted on the backup centers rather than the active sites – they are libel to be not as effectively defended.) Additional hardening of a single site may be more cost-effective than a backup center. Additional “hardening” is also provided by the elasticity and inertia of the system. An analysis such as that above, coupled with power stability studies would be necessary to determine the true need for a backup control center.</p>	The standard has been modified as suggested.

Name	Company	Comments	Drafting Team Responses
Dennis Kalma	AESO	<p>1308.a.1 90 days would be consistent with other sections and more reasonable.</p> <p>1308.b.1 90 days would be consistent with other sections and more reasonable.</p>	1308.a.1/1308.b.1 The standard has been modified.

Name	Company	Comments	Drafting Team Responses
Ed Goff	Progress Energy	<p>1308</p> <p>Recovery Plans [page 34] - and generation plants that have no critical cyber assets - Is this possible? What criteria are used to make this determination? If the criteria are included in the document, it should be referenced here at the least.</p>	The standard has been modified.

Name	Company	Comments	Drafting Team Responses
Ed Riley	CAISO	<p>1308 The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies.</p> <p>1308.a.1 Post is misleading and suggest posting to a broad audience. It should be modified to reflect its real nature which is publishing to documents that only individual with a need-to-know would use in an event of a crisis.</p> <p>Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand.</p> <p>The last paragraph is very wordy and could be reworded to be clearer.</p>	<p>1308 The introduction paragraphs has been modified.</p> <p>1308.a.1 The standard has been modified to clarify the drafting team's intent. FAQ has been updated.</p> <p>Testing has been moved to the FAQ.</p> <p>The last paragraph has been moved to the FAQ.</p>



Name	Company	Comments	Drafting Team Responses
Ed Stein	FirstEnergy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34:  1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security.  “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.  Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>The standard has been modified. References to posting have been removed.</p>

Name	Company	Comments	Drafting Team Responses
		<p>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</p> <p>2. ABC does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</p> <p>ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
Francis Flynn	National Grid	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Gary Campbell		<p>1308</p> <p>Measures</p> <p>1 I suggest the statement be changed to " The responsible entity shall have recovery plans and maintain ....." This is simple and to the point.</p> <p>2 It is hard to measure "as necessary". This should be dropped.</p> <p>3 The term " at least once every three years or as necessary" should be removed. Training records as required by P8T3 should maintained and auditable on an on-going basis. This requirement should keep with that language.</p> <p>Levels of noncompliance</p> <p>1 Adequately is to vague of a term. If the items in sentence two are important then they should be needs to defined in requirement and measured with a definitve measure.</p> <p>2 Need to reword the term " performed appropriately" is to vague and carries many meanings.</p> <p>3 Where in the document can the CM find the types of events that are necessary?</p>	<p>Measures</p> <p>1 The existing language has been retained.</p> <p>2 The standard has been modified. .</p> <p>3 Modified</p> <p>Levels of noncompliance</p> <p>1 The term adequately has been removed.</p> <p>2 The term " performed appropriately" has been removed.</p> <p>3 The types of events that are necessary are not defined in the standard. Thet are based on individual entities' risk assessments.</p>

Name	Company	Comments	Drafting Team Responses
Guy Zito	NPCC	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Jim Hiebert	WECC EMS WG	<p>The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies.</p> <p>Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand.</p> <p>The last paragraph is very wordy and could be reworded to be clearer.</p>	1308 The standard has been modified for clarity and consistency. It will be reformatted.

Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34:  1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security.  “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.  Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>The standard has been modified. References to posting have been removed.</p>

Name	Company	Comments	Drafting Team Responses
		<p>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</p> <p>2. ABC does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</p> <p>ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	



Name	Company	Comments	Drafting Team Responses
Karl Tammer	ISO-RTO Council	<p>This introduction is repetitive and redundant. It could be shortened to one paragraph and still be effective.</p> <p>1308.a(3): “Post” is misleading and suggests posting to a web site or similar. It should be modified to reflect its real nature, which we feel is publishing to documents that a team would use in a crisis.</p>	The standard has been modified. References to posting have been removed.

Name	Company	Comments	Drafting Team Responses
Kathleen Goodman	ISO-NE	<p>1308 Preamble</p> <p>1. This introduction is repetitive and redundant. It could be shortened to one paragraph and still be effective.</p> <p>2. To remain consistent with the scope of “Critical Cyber Assets,” it should be more clearly stated that this section only speaks to the operative recovery of those Critical Cyber Assets.</p> <p>1308 Requirements</p> <p>(3) What does "post" mean? This information could be considered confidential, protected, etc, etc...</p>	<p>1. The standard has been modified.</p> <p>2. Clarity has been added.</p> <p>3. References to posting have been removed.</p>

Name	Company	Comments	Drafting Team Responses
Ken Goldsmith	Alliant Energy	<p>308 Recovery Plans</p> <p>Article a-3 Updating recovery plans within 30 days of system change is unreasonable. Should just state recovery plans are to be maintained.</p>	Article a-3 has been modified.

Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	<p>Section 1308</p> <p>(text)(1st parag.) – The first sentence, by listing only certain entities, appears to exclude generation and transmission owners. They should be included. The sentence should begin: “The responsible entity must establish...”</p> <p>(text)(3rd parag.) – Move this entire paragraph to the FAQ, as it merely explains the meaning or intent of the standard. Also the second sentence appears to make a requirement by using a phrase that includes the word “require.” That it is intended instead to be merely explanatory is supported by the fact that there is no reference to redundant/backup facility in the “Requirements” or “Measures” subsections. Therefore, revise the sentence (even if relocated to the FAQ) to read “one control center per bulk transmission service area, often with a redundant or backup facility.”</p> <p>(a)(1) – To make this consistent with the third sentence of the second paragraph in the text portion of this standard, this should be revised to read (in part) “exercise its recovery plans annually where there is a low probability of a severe-consequence event.”</p> <p>(a)(3) – As worded, this is confusing, overly prescriptive, and unclear. It should read “The responsible entity shall maintain and communicate to all appropriate personnel an up-to-date recovery plan, including all necessary contact and communication information.”</p>	<p>(text)(1st parag.) Modified</p> <p>(text)(3rd parag.) Moved to FAQ</p> <p>(a)(1) has been modified.</p> <p>(a)(3) has been modified.</p>

Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34:  1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security.  “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. Cinergy seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.  Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>The standard has been modified. References to posting have been removed.</p>

Name	Company	Comments	Drafting Team Responses
		<ol style="list-style-type: none"> <li>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</li> <li>2. Cinergy does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. Cinergy regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</li> </ol> <p>Cinergy recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
Laurent Webber	WAPA	This comment also applies to 1308 Recovery Plans (a)(4): Reference 1303, Personnel and Training (1)(2)(iv) - Training on recovery of critical cyber assets should be tied to the system or structure (Under NIST this is part of the Security Plan) and not general Cyber Security Awareness training.	The standard has been modified.

Name	Company	Comments	Drafting Team Responses
Linda Campbell	FRCC	<p>1308 Recovery Plans</p> <p>The standard's purpose is Cyber Assets protection. In paragraph 1, we suggest changing "must establish recovery plans" to "must establish critical cyber asset recovery plans."</p> <p>The language of paragraph 3 section appears to be expanding the scope well beyond the recovery of the cyber assets. Suggest removing the entire paragraph. This standard does not deal with recovering substations, generating plants, nor control center facilities.</p> <p>(a) (3) "and post its recovery plan contact information" – post where?? For who? And why?</p> <p>(a) (4) delete "that will be included in the security training and education program" and replace with "that will be provided to personnel with a role in the recovery"</p> <p>(b) (2) change to "and adjust, if warranted, its response"</p> <p>(d) (3) numbered references are incorrect</p> <p>(e) (3) does not address "the types of events that are necessary" – this is very vague, please be more specific about what you mean.</p>	<p>Paragraph 1 has been modified and paragraph 3 moved to the FAQ.</p> <p>(a) (3) References to posting have been removed.</p> <p>(a) (4) has been modified.</p> <p>(b)(2) hs been moved to the FAQ</p> <p>(c) (3) the standard will b reformatted.</p> <p>(e) (3) Specific assets are determined by Entity Risk Assessment.</p>



Name	Company	Comments	Drafting Team Responses
Michael Anderson	Midwest ISO	<p>Business Continuity Can this section be modified to include plans that are not developed around particular assets instead of being developed for critical business functions?</p> <p>The continuity plans address if some or all of the critical functions are lost for an extended period of time, on how the business must react to maintain system wide safety and reliability in varying conditions. They do not particularly address any one critical asset. Can assets be more directly addressed?</p> <p>Also the alteration or change out of a particular asset does not always warrant a change to a function that is addressed within a particular business continuity plan. Why would a procedural change require posting of new contact information? It may require some alteration to a particular contingency plan but would not necessarily warrant making any change to contact information.</p>	<p>The Business Continuity section has been modified.</p> <p>The standard does not address specific assets as they are determined by individual entities' risk assessments.</p> <p>References to posting contact information have been removed.</p>

Name	Company	Comments	Drafting Team Responses
Paul McClay	Tampa Electric Company	<p>1308 Recovery Plans</p> <p>The standard's purpose is Cyber Assets protection. In paragraph 1, we suggest changing "must establish recovery plans" to "must establish critical cyber asset recovery plans."</p> <p>The language of paragraph 3 section appears to be expanding the scope well beyond the recovery of the cyber assets. Suggest removing the entire paragraph. This standard does not deal with recovering substations, generating plants, nor control center facilities.</p> <p>(a) (3) "and post its recovery plan contact information" – post where?? For who? And why?</p> <p>(a) (4) delete "that will be included in the security training and education program" and replace with "that will be provided to personnel with a role in the recovery"</p> <p>(b) (2) change to "and adjust, if warranted, its response"</p> <p>(d) (3) numbered references are incorrect</p> <p>(e) (3) does not address "the types of events that are necessary" – this is very vague, please be more specific about what you mean.</p>	<p>Paragraph 1 has been modified and paragraph 3 moved to the FAQ.</p> <p>(a) (3) References to posting have been removed.</p> <p>(a) (4) has been modified.</p> <p>(b)(2) hs been moved to the FAQ</p> <p>(c) (3) the standard will b reformatted.</p> <p>(e) (3) Specific assets are determined by Entity Risk Assessment.</p>

Name	Company	Comments	Drafting Team Responses
Pedro Modia	FPL	<p>(a)(3) Please explain “Post.”</p> <p>Further clarification is required in regards to “investigations upon complaint.” How intrusive are these investigation, and what would predicate such investigations?</p>	<p>References to posting have been removed.</p> <p>Depth and breadth of NERC compliance investigations are not covered in this standard and are defined in NERC's Compliance Program.</p>

Name	Company	Comments	Drafting Team Responses
Ray A'Brial	CHGE	<p>In 1308, to remain consistent with the scope of critical cyber assets, it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>1307 &amp; 1308- Response &amp; Recovery Plans</p> <p>Page 34:  1300 Language seems to imply NERC expects multiple plans to be created for Cyber Security.  “ ...recovery plans associated with control centers will differ from those associated with power plants and substations.” This level of detail may become too onerous. ABC seeks clarification from NERC if multiple plans are required. Once again, this will involve time, money and resources to create documentation at an unprecedented detail level with no indication that such a measure will increase real security.</p> <p>If entities strictly follow the language proposed for 1307, they will be forced to create un-necessary documentation for very brief interruptions and for events, which were not malicious and did not create a disruption. NERC definitions provided the following:</p> <ul style="list-style-type: none"> <li>• NERC defines an “incident” as ANY physical or cyber event that disrupts or could lead to a disruption of the critical cyber assets.</li> <li>• Same section defines a “cyber security incident” as malicious or suspicious activities, which cause or may cause an incident.</li> <li>• Definition section does NOT include a definition of a “reportable incident”</li> </ul> <p>The language of the entire 1307 section is written to apply to both incidents and cyber security incidents.  Once again, as we have seen in other sections, companies that attempt to follow these requirements will create costly levels of detail and documentation (for every incident which either creates a slight disruption or could lead to a disruption) with no proven direct benefit to security. Here are some examples:</p> <ul style="list-style-type: none"> <li>• Page 32 states, “...retain records of incidents and cyber security incidents for 3 calendar years.” This includes but is not limited to: <ul style="list-style-type: none"> <li>o System and application log files</li> <li>o Video and or physical access records</li> <li>o Investigations and analysis performed</li> <li>o Records of any action taken including recovery actions</li> <li>o Records of all reportable incidents and subsequent reports</li> </ul> </li> <li>• ...make all records and documentation available for inspection.”</li> </ul> <p>Recommendation: Re-work the language so that it is clear at what level this degree of detailed documentation needs to be retained.</p> <p>Page 34 (a) (3) “...update the recovery plans within 30 days of a system or procedural change and post the recovery plan contact information.” This language is problematic in 2 areas:</p>	<p>The standard has been modified. References to posting have been removed.</p>

Name	Company	Comments	Drafting Team Responses
		<p>1. It is not realistic to expect that the plan will be updated within 30 days of each procedural or system change.</p> <p>2. ABC does not “post” contact information. NERC does not specify what type of “posting” they require. Further this requirement is contradictory to other NERC cyber security requirements. ABC regards emergency plans and contact information as critical cyber asset information. Information is treated as such.</p> <p>ABC recommends that plans be updated annually and that contact information should be treated consistent with other information related to critical cyber assets.</p>	

Name	Company	Comments	Drafting Team Responses
Richard Engelbrecht	Rochester Gas & Electric	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	<p>Section 1308: The first sentence in the first paragraph does not list transmission owner or generator owner. Were these omitted on purpose? The last two sentences of second paragraph conflict with 1308.a.1 requirement (i.e. a higher probability event with a short duration may not require a recovery plan at all versus the requirement of annually tested recovery plan). The third paragraph states that this will require a redundant or backup facility regarding a control center. Is this a requirement for a redundant EMS/SCADA system? If yes, it is not listed in the requirements or measures. This should be clarified.</p> <p>Section 1308.a.3: This section states that a responsible entity shall update its recovery plans within 30 days of system or procedural change as necessary and post its recovery plan contact information. What is meant by post (e.g. external internet, internal)?</p>	<p>The first and second paragraphs have been modified.</p> <p>The third paragraph has been moved to the FAQ.</p> <p>References to posting have been removed.</p>



Name	Company	Comments	Drafting Team Responses
Robert Pelligrini	United Illuminating	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Robert Strauss	NYSEG	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>1308 Recovery Plans, Introductory Text</p> <p>Much of this text particularly the third paragraph is instructional and/or clarifying and is not consistent with other standards being developed as far as requirement introduction. It either belongs in a requirement and/or in a reference document such as the FAQ or other supporting document.</p> <p>(2nd paragraph) – Delete and add “Conduct required exercises annually”. Paragraph is too long and confusing.</p>	<p>The first and wsecond paragraphs have been modified. The third paragraph has been moved to the FAQ.</p>

Name	Company	Comments	Drafting Team Responses
S. Kennedy Fell	NYISO	<p>In 1308, to remain consistent with the scope of "critical cyber assets", it should be more clearly stated that this section only speaks to the operative recovery of those critical cyber assets.</p> <p>Following this concept, the third paragraph in the 1308 preamble should be removed. Backup and recovery of Control Centers is covered by other NERC Standards.</p>	<p>Clarity has been added.</p> <p>The paragraph has been removed.</p>

Name	Company	Comments	Drafting Team Responses
Stacy Bresler	Pacifcorp	1308 plans must address triggering events of varying duration and severity in the context of this paragraph calls into question whether this means different plans for different severities, and different durations, rather than one plan that addresses varying durations and severities. Please clarify.	Modified. Moved to FAQ

Name	Company	Comments	Drafting Team Responses
Terry Doern	BPA	<p>An alternative wording for this section is: Entities must perform business impact analysis that results in emergency response, disaster recovery, and continuity of operations plans as appropriate to the entity.</p> <p>BPA Transmission is in agreement with the WECC EMS WG's comment: The introduction paragraphs read more like requirements and should be in the appropriate section. Goes back to the formatting inconsistencies.</p> <p>Annual testing of low probability events is to frequent, focus on training our operators on higher probability events has more value and allows them to focus on the job at hand.</p> <p>The last paragraph is very wordy and could be reworded to be clearer.</p>	<p>The language regarding business impact analysis has been retained.</p> <p>The introduction paragraphs have been modified</p> <p>Annual testing of low probability events has been moved to FAQ.</p> <p>The last paragraph has been modified.</p>

Name	Company	Comments	Drafting Team Responses
Tom Flowers	Centerpoint Energy	<p>Page 34, 1308 Recovery Plans Introduction: Replace the first sentence with this "The responsible entity must establish recovery plans and put in place the physical and Cyber assets necessary to put these recovery plans into effect once triggered."</p> <p>Delete the third paragraph. Create a Frequently Asked Question. (FAQ) out of this paragraph.</p> <p>(a)(1) Requirements Replace (1) with "The responsible entity shall create Recovery Plans for critical Cyber assets and exercise its Recovery Plans at an appropriate periodicity."</p> <p>(a)(3) Replace (3) with "The responsible entity shall update its Recovery plans as soon as possible after a significant system or procedural change and redistribute the revised plans appropriately."</p>	<p>The introduction has been modified. The third paragraph has been moved to the FAQ.</p> <p>The requirements have been modified.</p>

Name	Company	Comments	Drafting Team Responses
Tom Pruitt	Duke Energy	<p>1308 The language in the introduction "...will require a redundant or backup facility" is not included in the requirements or measures section. Clarify whether this is a requirement. Why exclude Transmission Owner and Generation owner from the requirements of this section?</p> <p>What does "post its recovery plan contact information" mean as is used in requirement 3?</p> <p>1308(a)(1) Annual exercise for each system is not warranted. 1308(b)(1) To whom will the report be submitted?</p>	<p>1308 The language in the introduction has been removed.</p> <p>The requirements have been modified.</p> <p>References to posting have been removed.</p> <p>1308(a)(1) Please see further explanation in FAQ</p> <p>1308(b)(1) Standard does not address submittal</p>



Name	Company	Comments	Drafting Team Responses
Tony Eddleman	NPPD	Section 1308 Recovery Plans requires physically and cyber assets not currently required by NERC Template P6T3, Emergency Operations / Loss of primary Controlling Facility. The two should be consistent.	The section has been revised for consistency.

Name	Company	Comments	Drafting Team Responses
William Smith	Allegheny Energy	<p>1308 Recovery Plans</p> <p>1308.paragraph 3: This paragraph belongs in the FAQ instead of the standard and should be removed, rewritten and clarified.</p> <p>1308.paragraph 3: The first sentence of this section potentially contradicts the last sentence. In a power station, indeed a severe enough problem will lead to reconstruction of more than just the cyber assets. This paragraph should be more specific on what is required. Power station cyber assets should have sufficient plans to recover from system loss due to equipment failure, malfunction, or other failure. Plans for reconstruction because of catastrophic plant failure should not be required since more complete redesign and reconstruction of the entire plant may be required that cannot be planted for. Revise the standard to indicate this.</p>	The third paragraph has been modified and moved to the FAQ.

## Additional Comments and Drafting Team Reponses

Name	Company	Comments	Drafting Team Responses
Ed Stein	FirstEnergy	<p>FAQ's Recently Posted by NERC</p> <p>In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "...have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command..." As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.</p> <p>ABC Implementation Timeline</p> <p>After the Standard 1300 language and requirements are finalized, ABC estimates:</p> <ul style="list-style-type: none"> <li>o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.</li> <li>o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.</li> <li>o 3.5 to 4 years to implement and become compliant.</li> <li>o Total of 5 to 6 years from acceptance of the standard until compliance is reached.</li> </ul>	<p>The FAQ provide additional clarity and attempt to provide insight to the drafting team's rationale regarding the requirements and measures.</p> <p>A draft implementation plan will be posted with draft version 2 of the standard.</p>

Name	Company	Comments	Drafting Team Responses
Greg Fraser	Manitoba Hydro	<p>FAQ Section 1304 Question 7: I have a Virtual Private Network (VPN) that allows some external computers to connect to a VPN server on my security perimeter. Have I extended my security perimeter?</p> <p>The electronic security perimeter is extended to include the remote end unless the VPN access goes through firewall. VPN does not extend the electronic security perimeter if appropriate access controls implemented at the VPN server. 1st generation IPSEC VPNs tend to be an encrypted pipe allowing all ports with no current mature technologies to ensure the security of the remote end.</p> <p>After the standard drafting team is disbanded, who will respond to any questions regarding interpretation of the cyber security standard?</p>	

Name	Company	Comments	Drafting Team Responses
Howard Ruff	WE Energies	<p>Compliance will have a financial impact for entities covered by the standard.</p> <p>Identification of bulk electric system assets and performing a risk analysis with documentation will require resources and time to complete. Full compliance may not be achievable in the near term. NERC should keep the scope of what's included as critical cyber assets the same as interim standard 1200 until we gain more experience with compliance and certification.</p> <p>Who is going to determine whether an entity has defined their Critical Cyber Assets and Bulk Electric System Assets appropriately?</p>	<p>The scope of this standard was determined by public review and comment during the Standards Authorization Request process. The approved SAR is available from NERC's web site.</p> <p>For the purposes of this standard, the quality of the risk assessment method used to identify critical cyber assets will not be judged, only that one has been used.</p>

Name	Company	Comments	Drafting Team Responses
Joanne Borrell	First Energy Services	<p>FAQ's Recently Posted by NERC</p> <p>In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "...have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command..." As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.</p> <p>ABC Implementation Timeline</p> <p>After the Standard 1300 language and requirements are finalized, ABC estimates:</p> <ul style="list-style-type: none"> <li>o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.</li> <li>o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.</li> <li>o 3.5 to 4 years to implement and become compliant.</li> <li>o Total of 5 to 6 years from acceptance of the standard until compliance is reached.</li> <li>o of the standard until compliance is reached.</li> </ul>	Please see the reponses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Larry Brown	EEI Security Committee	The FAQs need to be cleaned up and made completely consistent with the standard.	The FAQs will be reviewed for consistency.

Name	Company	Comments	Drafting Team Responses
Larry Conrad	Cinergy	<p>FAQ's Recently Posted by NERC</p> <p>In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "...have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command..." As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.</p> <p>Cinergy Implementation Timeline</p> <p>After the Standard 1300 language and requirements are finalized, Cinergy estimates:</p> <ul style="list-style-type: none"> <li>o1.5 to 2 years to evaluate standard impact and what is to be included in compliance.</li> <li>oThis is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.</li> <li>o3.5 to 4 years to implement and become compliant.</li> <li>oTotal of 5 to 6 years from acceptance of the standard until compliance is reached.</li> </ul>	Please see the response to Ed Stein.



Name	Company	Comments	Drafting Team Responses
Laurent Webber	WAPA	<p>Generally agree with the thoughts and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. Will there be an expanded implementation timeframe in which to address the standard (beyond first quarter 2006)?</p> <p>Also, a general comment that the standard requires a significant amount of diligence (especially in the tracking, authorization, and management of sensitive information) and will undoubtedly lead to staffing increases.</p>	<p>A draft implementation plan will be posted with draft version 2 of the standard.</p>

Name	Company	Comments	Drafting Team Responses
Lloyd Linke	WAPA - MAPP	Generally agree with the thought and principles behind the new standard; however, are concerned about the considerable expansion in the number and types of critical cyber assets, as well as the increased specificity throughout the standard. The standard requires a significant amount of diligence (especially in the tracking, authorization and management of sensitive information) and will undoubtedly lead to staffing increases.	A draft implementation plan will be posted with draft version 2 of the standard.

Name	Company	Comments	Drafting Team Responses
Ray Morella	First Energy	<p>FAQ's Recently Posted by NERC</p> <p>In addition to inserting requirements regarding separation of duties noted above, question 3 on page 9 of the FAQ document seeks to limit the definition of RTU's, that use a non-routable protocol. Standard 1300 implies that non-routable protocols are excluded. However, the answer to question 3 tightens the definition of what is excluded by adding additional requirements that may not apply to all non-routable protocols: "...have a master/slave synchronous polling method that cannot be used to access anything on the EMS and they use SBO command..." As noted above, it is not appropriate to introduce additional restrictions to the Standard language via the FAQ posting process.</p> <p>ABC Implementation Timeline</p> <p>After the Standard 1300 language and requirements are finalized, ABC estimates:</p> <ul style="list-style-type: none"> <li>o 1.5 to 2 years to evaluate standard impact and what is to be included in compliance.</li> <li>o This is dependent upon how much guidance is given by NERC in regards to specifics for equipment and facilities to be included.</li> <li>o 3.5 to 4 years to implement and become compliant.</li> <li>o Total of 5 to 6 years from acceptance of the standard until compliance is reached.</li> </ul>	Please see reponses to Ed Stein.

Name	Company	Comments	Drafting Team Responses
Richard Kafka	PEPCO	FAQ Section 1304, question 1: The addition of dial-up connection to relays and RTUs using both routable and non-routable protocols should be added to the diagram. The diagram would be a useful addition to the actual standard.	

Name	Company	Comments	Drafting Team Responses
Roman Carter	Southern Company	<p>Comments from FAQs " Frequently Asked Question Document"</p> <p>Question 8, Section 1301 -- If the "separation of duties" is an important consideration as is implied in the "Answer" to this question then it should be added to the requirements.</p> <p>-- Frequently Asked Question Document -- Question 2, Section 1306 -- Bullet 4 ("Performance testing to assure system stability under load conditions") is not a cyber security issue and should be removed.</p> <p>-- Frequently Asked Question Document -- Question 8, Section 1306 -- The answer references what appears to be an incorrect preceding question.</p>	<p>The FAQs will be reviewed in concert with the requirements.</p>

Name	Company	Comments	Drafting Team Responses
Russell Robertson	TVA Transmission	<p>TVA is concerned that this version of the standard will reach well beyond the boundaries of the Urgent Standard. For instance, certain of the generation facilities could be deemed 'critical' by the Reliability Coordinator, but there is no clear evidence that the generation owner segment has paid particular heed to this standard (the original standard clearly targeted system operation centers, not external facilities). TVA urges the standard team to seek dedicated input to the process from generation owners who might be affected (for example, being designated as a DCS level unit by the Reliability Coordinator). Earlier comments dealt with the comparison of this standard with other industry requirements to ensure a consistent approach, and this is still a concern in the industry.</p>	<p>The drafting team understands the concern and urges all entities to take part in NERC's standard development process and, specifically, to provide comments during the public review and comment periods.</p>

Name	Company	Comments	Drafting Team Responses
Scott McCoy	Xcel Energy	<p>NERC should lean on existing standards including National Institute of Standards and Technology (NIST) Cyber Security standards (See series 800, Computer Security) that are already well-developed and tested, instead of having electric utility people create a whole new set of such standards. Also, as a general comment, the NERC standard seems to have redundancy with other security compliance requirements such as Sarbanes-Oxley, etc, but seems not to be well coordinated with these other standards. Would the NERC standard be served more efficiently if based on existing Cyber Security standards?</p>	<p>The drafting team has consulted existing best practices from NIST, ISO 17799, etc. And incorporated the intent into its draft standard. However, the requirements are intended to reflect the electric industry environment and experience.</p>

Name	Company	Comments	Drafting Team Responses
Seiki Harada	BC Hydro	<p>BC Hydro continues to support NERC's effort to represent the North American electricity industry in standard setting, and to help uphold the reliability of bulk electric systems via implementation of a set of cyber security standards.</p> <p>The acceptance of the NERC functional model (that describes the roles and responsibilities of entities such as Reliability Authority, Balancing Authority, Buying/Selling Entity, etc.) is essential to the implementation of the compliance monitoring. If the model was not endorsed nor implemented by NERC, the NERC 1300 standards may become a voluntary compliance guide, rather than standards.</p>	The drafting team appreciates these comments.