NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Frequently Asked Questions

CIP Version 5 Standards
Consolidated Comments Received Regarding April 1, 2015 Posting

This draft document is designed to provide answers to questions asked by entities as they transition to the CIP 5 Reliability Standards. It is not intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing reliability standards, nor provide an Interpretation under Section 7 of the Standard Processes Manual. Additionally, there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

This document consolidates industry feedback on the draft answers listed below that were received by NERC on the FAQs posted for comment on April 1, 2015 and due to NERC by May 15, 2015. NERC will review all comments provided and incorporate changes before issuing a final version.

General Comments – April 1, 2015 Posting

Organization	Comment
Puget Sound Energy	Puget Sound Energy supports the comments provided to NERC by the Edison Electric Institute
Kansas City Power & Light Company	Kansas City Power & Light Company supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
Edison Electric Institute (EEI)	We recommend that NERC add the disclaimer used with the Lessons Learned supporting documents that make it clear that the document is not intended to establish new requirements, modify the requirements, or provide an official interpretation. The disclaimer also clearly acknowledges that "there may be other

General Comments – April 1, 2015 Posting	
Organization	**Comment**
	legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document” and that compliance is based on the language of the standard. The use of “must” in many of the responses is concerning in these FAQs because it implies that this supporting document is a requirement or interpretation of the standard. To address this concern, we attempted to address this in our recommended rewordings in the specific comments below. However, we did not comment on every use of “must.” Therefore in general, we suggest removing “must” from all of the responses. Although the use of “should” is not as strong as “must,” we recommend limiting its use as much as possible. Some of the questions and answers below refer to versions of the CIP standards that have not yet been approved by FERC. For example, the answer to no. 83 uses CIP-006-6, which has yet to be approved. However, the question for no. 83 is inconsistent with the answer and uses CIP-006 and CIP-006-5. We recommend that NERC uses the existing, approved versions of the standards (e.g., -5 or -1) and then update the FAQs when the version of the standard changes (e.g., when FERC approves CIP-006-6). We have followed this recommendation in our comments below when we make recommendations to the change the text. We recommend that all of the FAQs—including those previously posted (November 25, 2014) as well as those below and others posted on May 1—be combined into one document as approved by the Standards Committee under Section 11 and organized by standard (including version) to make them easy to review by all stakeholders and update in the future. We also recommend making them available in a sortable format, e.g., Microsoft Excel. Finally, for each FAQ, include the date it was approved by the Standards Committee under Section 11.
Avista Corporation	Avista Corporation supports the Edison Electric Institute’s (“EEI”) comments on the CIP Version 5 Standards Frequently Asked Questions (“FAQs”) posted for comments on April 1, 2015, with comments due by May 15, 2015. Avista agrees with EEI that NERC should make clear that the FAQs and answers do not imply mandatory and enforceable requirements or interpretations of the CIP Version 5 Reliability Standards. Further, NERC should make clear that the FAQ’s and answers should not imply mandatory and enforceable

General Comments – April 1, 2015 Posting	
Organization	**Comment**
	requirements or interpretations under CIP Version 3 Standards to the extent there are CIP Version 5 Standard Requirements that closely map to the CIP Version 3 Standard Requirements. Regarding the content of FAQ answers, where NERC wishes to convey examples of what may constitute appropriate evidence or implementation strategies, NERC should clearly state them as examples or best practice so that they are not misinterpreted as requirements. Avista also agrees with EEI that the FAQs and answer should be combined into one document. Organizing the FAQs by Standard and/or subject matter would greatly improve the ease in referencing this guidance document. Avista applauds NERC's efforts to provide Industry this important guidance during the CIP Version 5 Transition Period and appreciates the opportunity to provide these comments.
PSEG	PSEG supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
PacifiCorp	PacifiCorp appreciates the opportunity from NERC to provide substantive review and comment on the draft of the CIP Version 5 Frequently Asked Questions, dated April 1, 2015. Along those lines, PacifiCorp commends NERC for forming the CIP Version 5 Advisory Group, and that group for developing answers to questions frequently asked by entities seeking to comply with the CIP Version 5 requirements. In looking to provide answers that reflect the lessons learned through the process of complying, PacifiCorp supports the Edison Electric Institute comments submitted on May 15, 2015, and requests that NERC consider them when reviewing whether modifications should be made prior to posting the document as final
Southern	Southern appreciates NERC efforts to develop and post for comment information that aids stakeholders in the implementation and understanding of the CIP Version 5 Standards. Southern supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
Oncor Electric Delivery, Inc.	Oncor Electric Delivery, Inc. supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
Westar Energy	Westar Energy supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.

General Comments – April 1, 2015 Posting

Organization	Comment
Tampa Electric Company	Tampa Electric Company participated in the development of the comments with members of the Edison Electric Institute. We support the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions filed May 15, 2015 and request that these be addressed by the FAQ team prior to finalizing them for industry use.
United Illuminating Company	The United Illuminating Company supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
MidAmerican Energy Company	MidAmerican Energy Company supports the Edison Electric Institute comments on the CIP Version 5 Standards Frequently Asked Questions posted for comments on April 1, 2015, with comments due by May 15, 2015.
ERCOT	ERCOT requests that NERC publish all questions received and how the question was addressed (e.g., FAQ, Lesson Learned, Memo, etc.).
Dominion	• A cross-reference should be added to each FAQ linking the requirement and associated part of specified requirement to the question. • Consider grouping the FAQ questions pertaining to the same requirement(s) and/or part(s).

Note: The "number" column in the table below is not relevant to stakeholders and is only included as an organizational tool for NERC.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
22	Is RFC 1490 Protocol considered serial? Routable?	A communications protocol that contains a network address as well as a device address is typically defined as a routable protocol. TCP/IP is a routable protocol, and the IP network layer in TCP/IP provides this capability. The TCP/IP suite provides two transport methods. TCP ensures that data arrive intact and complete, while UDP just transmits packets. RFC 1490 is an encapsulation method for carrying network interconnect traffic over a Frame Relay backbone. If IP traffic is encapsulated in this protocol, then it would be considered to be a routable protocol. Frame relay itself is a communications protocol that creates Permanent Virtual Circuits (PVCs) to send traffic between locations. Once PVCs are created, the network communications more closely resemble layer 2 communications. Examples: 1. If it is bridged to operate similar to a VLAN, then it is routable (but may possibly be considered similar to a layer 2 switch). 2. If it is used as an end-to-end IP link, then it is routable (but is evaluated differently since it is layer 3). 3. It can also be considered a communication link transport media, but that doesn't really change anything. The entity would need to evaluate to see if the communications would qualify for exemption under Section 4.2.3.2 under CIP-002-5.

Organization	**Comments**

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td>EEI</td><td colspan="2">We support this question and answer.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports the response provided.</td></tr>
<tr><td>APS</td><td colspan="2">This question is quite specific. For an FAQ, it may be more helpful to provide a general answer to two separate questions: “What protocols are considered routable?” and “What attributes make any protocol considered to be routable? When the specificity gets to such a detailed level it implies that all answers are contained herein and runs the risk of excluding elements. Leaving questions at a slightly higher level allows for broader application.
Example #1 is confusing. VLANs by nature are designed to segment (or zone) network traffic. This LAN isolation is typically done using a switch capable of creating VLANs. For example, a set of switch ports is assigned to VLAN A. Another set of switch ports is assigned to VLAN B. By doing so, there are now 2 isolated “virtual” LANs that did not require physical separation using a router. We do not believe that the example statement “If it is bridged to operate similar to a VLAN” is relevant to determining if a protocol used at the BCA is routable or not.
Example #2 is confusing because of the parenthetical. This is likely an unnecessary statement.
Example #3 seems to be unnecessary. If it doesn’t change anything or relate to the determination if a protocol in use is routable or not then it should not be used in the Answer.</td></tr>
<tr><td>ERCOT</td><td colspan="2">ERCOT respectfully disagrees with the proposed response. RFC 1490 is not performing the routable communications. It is merely the transport means. The routability should be defined by a combination of other configuration parameters and the use of TCP/IP or another routable communication. ERCOT suggests that NERC revise the proposed response to provide greater consideration to the discrete roles of TCP/IP versus RFC 1490 identified above.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
23	Is IEC 61850 a routable protocol (for purposes of high and medium impact)?	IEC 61850 is an Ethernet-based standard for the design of electrical substation automation and the abstract data models can be mapped to a number of protocols, including MMS (Manufacturing Message Specification, the underlying communication architecture for ICCP), GOOSE, and Web Services. IEC 61850 is not a data link or network layer protocol, thus declaring IEC 61850 to be a routable or non-routable protocol is not appropriate. Time-critical messages, such as GOOSE messages for direct inter-bay communication, typically run on a flat Layer 2 network without the need for Layer 3 IP addresses. Other non-time-critical messages, including MMS and web services, typically run on a Layer 3 network, such as TCP/IP, with addressing and routing. The registered entity should carefully evaluate the communication environment supporting the IEC 61850 data protocol to determine if routable communication exists. If the IEC 61850 data is being communicated over a TCP/IP network, then that network connectivity is considered routable and should be protected per the CIP Standards accordingly. Note: Low impact requirements exempt 61850 from its scope.

Organization	Comments
EEI	We support this question and answer.
AEP	AEP supports the response provided.
APS	Please see comments on #22 above regarding specificity.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
MISO	In this FAQ, the question asks whether IEC 61850 is a routable protocol. The Comments state that "declaring IEC 61850 to be a routable or non-routable protocol is not appropriate," because IEC 61850 is "[neither] a data link or network layer protocol." We support the considerations made by the Committee. However, to remove ambiguity, we believe that IEC 61850 should be designated as a routable protocol given that it is generally deployed in a routable environment or, alternatively, that the standards somehow impact deployment of security protocols to protect non routable IEC 61850 traffic (i.e. IEC 62351-6). The Committee has chosen to give deference to a registered entity in deciding whether their use of IEC 61850 is routable or not. The making of such a determination relies on registered entities evaluating the communication environment to see if routable communication exists. This can be ambiguous and, at worst, can lead to a situation where an entity chooses to deploy IEC 61850 in a non routable manner without protecting this traffic because the standards do not require it.	
25	Should the identity management tool be classified as an EACMS? It will reside in an ESP DMZ environment and could be on a dedicated VM infrastructure.	The definition of Electronic Access Control or Monitoring Systems (EACMS) is "Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems." If the function of the identity management system is to capture and/or gather information pertinent to the attributes (e.g., biometrics) of a subject or data relevant to a subject, then perform a subsequent analysis or decision of the captured data to enforce access control (e.g., authentication and/or authorization) or monitoring of an Electronic Security Perimeter, then the identity management system should be considered an EACMS.
Organization	**Comments**	
Puget Sound Energy	Identity management and identity & access management systems can vary greatly in the actions that they perform. We feel that the single example of what would be an EACMS is insufficient to provide adequate guidance in determining whether or not the tool should be considered an EACMS. We feel a clearer definition of “access control” in the context of EACMS should be provided. Based on the answer provided, it appears that the intention is to consider a tool as an EACMS only if the tool provides the capture and analysis of identity information and the enforcement of access to a specific asset at the	

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td></td><td colspan="2">time the identity information is presented by the user in real-time (such as via a login screen or thumb print scanner). If a tool is not involved in the real-time control of access, that tool would not be considered an EACMS.

At a high level, the access control process could be described by the steps listed below:

1. An individual determines there is a need for access to an ESP or BES Cyber System
2. A request for access to the ESP or BES Cyber System is initiated
3. The request is presented to an authorized approver for approval or denial of the request
4. If approved, the identity information is configured on the appropriate EACMS
5. An individual presents their identity information to gain access to the ESP or BES Cyber System
6. The EACMS analyzes the presented identity information
7. The EACMS allows or prevents access based on the results of the analysis of the identity information

Systems and processes performing only steps 1 – 4 (above the line), which are typically done only once per individual, are not considered EACMS. Systems and processes performing any of the steps 5 – 7 (below the line) which are typically repeatable and done in real-time, are considered EACMS.</td></tr>
<tr><td>EEI</td><td colspan="2">Identity management tools vary and can be configured in many different ways that can result in different functions. Due to this issue, the answer may be more complex than indicated in this response. As a result, we do not believe a FAQ is an appropriate supporting document to address this question and recommend removing this question and answer.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports this comment and suggests that the same arguments apply to identity management tools associated with Physical Access Control Systems, i.e. identity management systems not involved in the enforcement of access control should not necessarily be considered a PACS or part of a PACS.</td></tr>
<tr><td>APS</td><td colspan="2">This question appears to situationally specific to a single configuration. Rewording in more general terms allows for broader application. The statement in the second sentence does not seem to be relevant to the question. Alternative question: “What functions would cause an identity management system to be classified as an EACMS?”</td></tr>
</table>

<table>
<tr><th colspan="4">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th colspan="2">Question</th><th>Answer</th></tr>
<tr><td colspan="2">Dominion</td><td colspan="2">Comment:
The inclusion of “authorization” is problematic.
A Cyber Asset by definition includes hardware, software, and data. At the software level, authorization privileges are associated with specific roles. Authorization may also be provided through tools such as Active Directory or an IDS. The response indicates that any BES Cyber Asset that also includes software that enforces access privileges also needs to be identified as an EACMS.
The term “access” needs to be limited to “authentication” to be in alignment with the Guidelines and Technical Basis of CIP-003 and with the CIP-004 standard, and CIP-007 R5.
Proposed Change:
The term “access” needs to be limited to “authentication”. The term “authorization” should be removed from the answer.</td></tr>
<tr><td>33</td><td colspan="2">When identifying BES Cyber Systems, what is the definition of adverse impact?</td><td>Per comments from the standards drafting team, an adverse impact is a negative effect on the reliable operation of the BES. (See bottom of page 60 in the comments link provided above.) Entities need to perform some work to determine situations that would have a negative (adverse) impact on their normal (functional) operations. While we can produce specific examples, every entity is different, so adverse impact may have a different meaning to each.</td></tr>
<tr><th colspan="2">Organization</th><th colspan="2">Comments</th></tr>
<tr><td colspan="2">North American Generator Forum (NAGF)</td><td colspan="2">The NAGF notes that correlation back to the BES Cyber System and BES Cyber Asset definitions in the NERC Glossary would help enhance this response.</td></tr>
<tr><td colspan="2">EEI</td><td colspan="2">We recommend changes to both the question and answer below.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
		For the question, we recommend rewording it to: “when identifying BES Cyber Systems, what is an adverse impact?” We are making this recommendation because the term “adverse impact” was intentionally not defined and it would be inappropriate for a supporting document to offer or imply a definition. For the answer, the dictionary definition (a common understanding) of adverse is causing harm or harmful. Therefore, it is reasonable to believe that an adverse impact is an impact that causes harm or is harmful. We believe this is clear and a citation to the record of the standards drafting team is not needed except to explain the intent. And when citing to the record, it should be quoted with the related context. We recommend rewording the response to: “The common, dictionary definition of adverse is harmful or causing harm. Negative is a synonym of adverse. Therefore an adverse impact is a harmful or negative impact. This is supported by the comments of the standards drafting team: “Another comment was that the term "adversely impact" should be defined. The drafting team responded that the term adequately conveys the meaning of an impact that has a negative effect on the reliable operation of the BES and therefore does not need to be added to the NERC Glossary of Terms.” (NERC Consideration of Comments, Cybersecurity Order 706 Version 5 CIP Standards, p 60, available at: http://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/C_of_C_Project2008-06_CIPv5_20120412_Final.pdf).”
ACES		Due to the critical impact in scope of a registered entity of the word, ‘adverse impact’, a Lessons Learned would have been the more appropriate response to this question rather than a short generic FAQ response. To say an ‘adverse response’ is a negative impact is redundant and provides no clarification. A response that included BES conditions such as impacts on frequency or voltage, impact on the ability of controllers to monitor, impacts resulting in a modification of plant operations, impact on the ability of the grid to recover from an event or unit failure would provide more guidance. Are we to assume that all answers to v5 questions are to come from SDT industry comments? What protections are there in that 188 page document that there are no conflicting statements?

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td></td><td colspan="2">A BES Cyber System can have a negative impact on an asset and the asset can have no impact to the BES. Shouldn’t the focus be, “does the cyber asset have a negative impact to the asset and the BES?”
And what if the negative effect is, for example, a power plant reduces its generation output some amount, but doesn’t go off-line? What if that is only 10 MW? At what point is it an adverse impact to the BES? Seems like this is highly conditional. Agree that more guidance would be helpful unless the answer is simply that adverse impact is any change to the condition of a BES Asset.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports the response provided.</td></tr>
<tr><td>Seminole Electric Cooperative</td><td colspan="2">NERC may want to specifically identify the difference (or at least that there is a difference) between adverse impact and Adverse Reliability Impact (a glossary term).</td></tr>
<tr><td>APS</td><td colspan="2">An FAQ should not attempt to provide a definition where there is none in the official NERC Glossary of Terms. Although comments from the standards drafting team may be a relevant point in developing a definition for the term “adverse impact”, it should not be relied upon as the final definition. An appropriate level of input from industry as a whole is needed to develop a usable definition and then it should be added to the NERC Glossary of Terms per normal process.
This phrase seems to be misstated – “…adverse impact is a negative effect on the reliable operation of the BES.” Per the BCA definition, it is an adverse impact on one or more Facilities, systems, or equipment…”
The last sentence of this answer does not seem to add value.</td></tr>
<tr><td>MISO</td><td colspan="2">The Standards Drafting Team (“SDT”) believes that “adverse impact” adequately conveys the meaning of an impact that has a negative effect on the reliable operation of the BES and therefore does not need to be defined. The SDT's unwillingness to provide a rigorous definition seems to indicate that “adverse impact” should not be defined in the absolute.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		However, the excessive ambiguity leaves a registered entity with a broad interpretation of "adverse impact," thereby leaving a standard definition to be created through enforcement precedence. There is no guidance that articulates what the lowest (or at least acceptable) threshold of negative effect may be which leaves the audit process to define it. For example, Adverse Reliability Impact includes for example, "frequency-related instability, [or] unplanned tripping of load or generation." This low bar includes something as small as frequency deviations to larger issues like line load needing to be shed. We would also like to point out that in the BES Cyber Asset Survey, NERC identified that "there were some inconsistencies in what entities considered to be adverse impact on reliable operations." (See Survey p. 18) If "adverse impact," is intended to have a low threshold then it can, and should be, easily articulated. We ask that the SDT provide more articulation about, or examples of "adverse impact."
ERCOT		ERCOT respectfully suggests that NERC provide additional clarification regarding its proposed response. Initially, the proposed response emphasizes negative impacts on the reliable operation of the BES, but the follow up statement emphasized negative impacts on the entity’s normal operations and is not focused on the BES. The potential negative impact on an entity’s operations may not translate to a negative impact to the reliable operation of the BES. Accordingly, clarification is recommended.
Dominion		Comment: This FAQ is non-responsive, changing the word “adverse” to “negative” does not answer the proposed question. Agree with the response that the Registered Entity has the ability to define this term. Proposed Change: The response should be limited to allowing the registered entity to define adverse impact.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
45	How do you define 1500 MW?	It is the net Real Power capability, which is the gross Real Power capability less any auxiliaries, station service, or other internal use of the output of generation units. The following should be used for determination of Net Real Power: • Any method approved by a Transmission Planner or Reliability Coordinator that is independent of the Generator Owner. • Industry accepted engineering studies of net generation output, such as may be required of market participants. • The highest aggregate net generation output for the prior two years from an entity's energy accounting software. Reference MOD-024/MOD-025 as an acceptable approach.

Organization	**Comments**
North American Generator Forum (NAGF)	The NAGF notes that the 3rd bullet should be preceding 12 calendar months, not two years, to remain compliant to CIP-002-5.1.
National Grid	As FAQ (#45) is currently presented, NERC has provided 3 alternative and equally acceptable methods for determining Net Real Power capability. National Grid appreciates NERC's continued recognition that there is often no one-size fits all methodology for Registered Entities. As such, we agree that each alternative, while having the potential to produce slight variations in the end result, is able to stand alone on its own merits for purposes of supporting the 1500 MW threshold. In order to avoid confusion, however, NERC should consider the inclusion of an "or" qualifier after each of the available options: "The following should be used for determination of Net Real Power: • Any method approved by a Transmission Planner or Reliability Coordinator that is independent of the Generator Owner; or, • Industry accepted engineering studies of net generation output, such as may be required of market participants; or,

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		• The highest aggregate net generation output for the prior two years from an entity's energy accounting software. Reference MOD-024/MOD-025 as an acceptable approach." With this important qualifier, it will be clear that a Registered Entity is able to utilize any one of the three equally satisfactory NERC identified methods for determining Net Real Power capability.
EEI		We recommend changes to both the question and answer below. For the question, we recommend changing it to "how is 1500 MW determined under CIP-002-5.1, Attachment 1, criterion 2.1?" Use of "define" or "definition" as we commented above is not recommended for non-defined terms in a supporting document. Also, a reference to the standard is helpful. For the answer, we make the following three recommendations: 1. Change the word "should" in the second sentence to "are examples that could" because the standard does not prescribe any or all of these methods for determining net Real Power capability, they are examples of approaches that can be taken. 2. Remove "that is independent of the Generator Operator" because this is not in the standard. It is unclear where this language came from as it is not in CIP-002-5.1 and therefore appears to modify the requirement. Other NERC standards provide possible methods. For example, FAC-008-3 requires the Generator Owner to have a method of determining their facility rating and make it available for inspection and technical review by a Transmission Planner and Reliability Coordinator, but does not require the method to be "independent of the Generator Owner." 3. Modify the third bullet point so that it does not prescribe the timeframe as "two" years or limit the type of software that companies could use to track the generation output. Specifically, we recommend changing the third bullet point to read: "the highest aggregate net generation output for prior year(s). Reference MOD-024/MOD-025 as an example of an acceptable approach."
ACES		Where does it say it has to be approved by the TP or RC in the standard? This is modifying the standard. Must all three conditions be met? In other words, does the TP and RC have to approve if industry accepted engineering studies are used?

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
		The third bullet is inconsistent with the plain language of 2.1 in CIP-002. 2.1 states clearly “preceding 12 months”. It does not say two years. MOD-024 is not yet approved by FERC and, thus, it is not appropriate to require its use at this juncture. The bottom line is that the GO needs to provide information using commonly accepted engineering practices to demonstrate the unit capability.
Dominion		Comment: Pertaining to the 3 bullet points and should be removed [sic] Proposed Change: The bullet points should be listed as – or -
Duke Energy		Duke Energy suggests changing the language in bullet number three above. The current language suggests the highest aggregate net generation output for the prior two years…We believe this language to be in error. We suggest changing the language to “highest aggregate net generation output for the prior 12 calendar months…” This language better aligns with the language used in Attachment 1 of CIP-002.
49	What is a “shared” BES Cyber System?	One that affects two or more BES Facilities, such as multiple generation units. Reference the use of "shared" in context as used in CIP-002-5.1, Attachment 1, impact rating criterion 2.1.
Organization		**Comments**
North American Generator Forum (NAGF)		The scope of the CIP requirement is being broadened to more than the language within the Standard in leveraging the BES Facility definition. “Shared” only appears in CIP-002-5.1 Attachment 1, Criterion 2.1 when referencing multiple generation units and CIP-002-5.1 Attachment 1, Criterion 2.2 when referencing multiple generation reactive resources. The NAGF would like to understand why BES Facilities is used in this context when not appearing in the Standard.
EEI		We recommend changing the answer to: “Shared” BES Cyber Systems are those that are associated with any combination of units in a single interconnection, as referenced in CIP-002-5.1, Attachment 1, impact rating criteria 2.1 and 2.2. For criteria 2.1 “BES Cyber Systems

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single interconnection.” For criteria 2.2: “BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1000 MVAR.”
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		The answer is correct but does not really answer any questions. Seminole suggests that NERC provide 2-3 examples. i.e. For generation units, a shared generation plant control system. It is important to provide additional comment on content of CIP-002-5 criterion 2.1 and the risks related to declaring a common BES Cyber System that touches multiple Facilities.
APS		An FAQ should not attempt to provide a definition where there is none in the official NERC Glossary of Terms. An appropriate level of input from industry as a whole is needed to develop a usable definition and then it should be added to the NERC Glossary of Terms per normal process. The CIP-002-5.1 Requirement R1: Impact Rating of Generation Resource Shared BES Cyber Systems Lesson Learned document has two references that could be used to provide a consistent definition for Shared BES Cyber System: • Pg. 3: “Identifying shared BES Cyber Systems involves detailed analysis that considers shared generating plant operational processes (e.g., air, water, steam, environmental, and fuel handling processes) and electronic connectivity.” • Footnote 4, Pg. 3: “Shared BES Cyber Systems are typically introduced through common connectivity between systems on multiple units or common generating plant operational processes that can affect more than one unit.”

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
Duke Energy		Duke Energy suggests removing the use of the term BES Facilities in the answer above. We feel that using the term broadens the context of the standard, and could bring into scope assets that were not originally intended to be included. We suggest using a combination of the generation criteria established in criterion 2.1 and 2.2.
50	What are “common mode vulnerabilities?” – i.e. a (physically) control room that can control multiple units, a substation/yard for a power plant	Any systems that can affect two or more BES Facilities, such as multiple generation units. A substation could affect the entire generation location if it were disabled and power was not able to be transmitted on the grid. Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities. Refer to the Generation Segmentation Lesson Learned document.

Organization	Comments
North American Generator Forum (NAGF)	The NAGF recommends removing this question and answer. The concept of physical proximity within a control room being considered within a “common mode vulnerability” received negative feedback when in the Generation Segmentation Lesson Learned and now has re-appeared here. This is a new concept that is currently not supported by any existing Standard or Guidelines and Technical Basis language. In addition, the “common mode vulnerability” language does not appear in the Standard and shouldn’t be subject to an FAQ. Only language or concepts within the Standard itself should be subject to Guidance and not the Guidance itself.
EEI	In the Guidelines and Technical Basis section of the standard the term “common mode vulnerabilities" is preceded by "BES Cyber Systems with..." These additional words in the standard point the reader to look at cyber systems and not all of the physical devices that could be out there. We recommend rewording of the answer to: "Any BES Cyber System that can affect two or more BES Facilities, such as multiple generation units. A BES Cyber System in a substation could affect the entire generation location if it was disabled and power was not able to be transmitted on the grid. Protection systems, fuel-handling systems, cooling water, and air systems are also examples that should be evaluated as common mode vulnerabilities. Refer to the Generation Segmentation Lesson Learned document."

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
		Also, there are some typos in the question: add a comma after i.e., and change “physically” to physical.
ACES		This needs to reference that 1500 MW. It is how it is used in the Guidelines and Technical Basis section of the standard on page 24.
AEP		AEP supports EEI comments.
APS		This response does not provide additional clarity and by inserting a substation example it has actually become more confusing than before. The term “Common Mode Vulnerability” (CMV) does not appear in the Standard requirements and is yet to be clearly defined. Assuming that a CMV is being used for illustration purposes then the application should be done at the Facility. Additionally, the Lessons Learned document referenced in this FAQ response hints that the application is at a cyber asset rather than a generation Facility. This potential conflict can be found where the lesson learned document discusses network separation and firewall controls.
Dominion		Comment: Common mode vulnerabilities should be focused on the Cyber Assets or Cyber Systems, not the physical location or proximity of the Cyber Systems. The question for FAQ 50, is based on the incorrect assumption, it implies that a physical location (control room) is common mode vulnerability. The response doesn’t correct the incorrect question. Proposed Change: Remove Control Room from the example or state Control Room is not a part of the Common Mode Vulnerability. Common Mode vulnerability should be focused on BES Cyber Assets/Systems and not the physical locations.

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td>Duke Energy</td><td colspan="2">Duke Energy recommends that the above question and answer be removed from the FAQ document. Common Mode Vulnerabilities are not a part of the standard. The above language appears to be from the basis document. The language in the FAQ document should be restricted to language providing guidance to the industry.</td></tr>
<tr><td>52</td><td>How can we show that there is not a 15 minute impact on BES (what evidence needs to be supplied)?</td><td>Reference the BES Cyber Asset Survey for an indication of the types of systems the Implementation Study participants identified.</td></tr>
<tr><th>Organization</th><th colspan="2">Comments</th></tr>
<tr><td>North American Generator Forum (NAGF)</td><td colspan="2">This specific question is not really answered in the Survey study and is left open-ended (auditors unclear on how to evidence). The NAGF reserves comment until such a time that an answer is provided as to the type of evidence that may need to be supplied to support the time-impact a Cyber Asset may have.</td></tr>
<tr><td>EEI</td><td colspan="2">This question and answer is confusing because the question asks something that is not required by the standard, i.e., to identify Cyber Assets that do not meet the BES Cyber System definition due to the 15 minute adverse impact. The proposed answer does not answer the question about evidence, but points to the BES Cyber Asset Survey. We recommend adding the following language prior to the existing answer to help clarify:

“CIP-002-5.1, R1 requires Responsible Entities to consider a listed set of assets and identify each of the high, medium, or low impact BES Cyber Systems using Attachment 1. The standard does not require entities to identify Cyber Assets (or provide evidence on Cyber Assets) that are not BES Cyber Systems. Therefore there is no requirement to “show that there is not a 15 minute impact on BES” and therefore evidence of this is not needed. The measure for R1, M1, provides examples of acceptable evidence to meet the R1 identification of high and medium impact BES Cyber Systems, including dated electronic or physical lists of the high and medium impact BES Cyber Systems.”</td></tr>
<tr><td>ACES</td><td colspan="2">The question asked for a list of evidence that a registered entity can provide, e.g. attestation, to prove that there was not a 15 minute impact to the BES. Please provide a page and paragraph that explains your response in the link to the BES Cyber Asset Survey.</td></tr>
</table>

<table>
<tr><th colspan="4">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th colspan="2">Question</th><th>Answer</th></tr>
<tr><td colspan="2">AEP</td><td colspan="2">AEP supports EEI comments.</td></tr>
<tr><td colspan="2">Seminole Electric Cooperative</td><td colspan="2">To quote the report (in isolation as many will read it)

Evidence for Determinations – One Implementation Study participant noted that because a determination of whether a Cyber Asset is a BES Cyber Asset often depends on the judgment of a subject matter expert, the type of documentation or evidence necessary to demonstrate the validity of the decision to an auditor is unclear.

To answer the question, NERC should refer to specific sections/pages. Alternatively, Seminole suggests that NERC directly answer the question “what evidence needs to be supplied”.</td></tr>
<tr><td colspan="2">APS</td><td colspan="2">This question is not written to address what might be considered a frequently asked question. A suggested modification to the question would be: “How can a utility demonstrate that a Cyber Asset, per the definition of a BES Cyber Asset, would not affect the reliable operation of the Bulk Electric System?”

The BES Cyber Asset Survey does not provide an adequate response to what would need to be supplied as evidence.</td></tr>
<tr><td colspan="2">MISO</td><td colspan="2">MISO supports the findings in the BES Cyber Asset Survey that "NERC should provide industry additional guidance to help ensure that responsible entities are properly and consistently applying the BES Cyber Asset definition." (See Survey, p. 4) As noted in the survey, "no two entities used the exact same process for identifying BES Cyber Assets."

We agree that additional guidance is needed to help with the practical application of the BES Cyber Asset definition.</td></tr>
<tr><td colspan="2">ERCOT</td><td colspan="2">ERCOT respectfully suggests that NERC revise its proposed response to focus on the documentation aspects of the question.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
Dominion		The question was not answered.
54	Where in the standards is the FERC Order 706 directive on joint ownership or joint use addressed?	Since one Registered Entity must be responsible for compliance, there will need to be an agreement (e.g., JRO, CFR, MOU) in place clearly stating which Registered Entity has responsibility. Guidelines and Technical Basis states: "It is recommended that each BES Cyber System should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards." There is not an obligation in the CIP standards to have JROs, CFRs, or MOUs. Registered Entities can also get best practices ideas from peer forums, such as the Transmission Forum, the Generator Forum, and/or regional compliance forums.
Organization		**Comments**
EEI		The phrase “there will need to be an agreement” implies an additional requirement. We recommend removing the first sentence and adding a reference to CIP-002-5.1 prior to “Guidelines and Technical Basis” so that it is clear which standard is being referenced.
ACES		NERC and the regions supposedly have a database identifying who is registered for BES Asset (i.e. generating plant, substation, etc). Why can’t they use this to figure out who is responsible?
AEP		AEP supports EEI comments.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
Seminole Electric Cooperative	This question is inadequately addressed. For specific examples, contact the FRCC CIPS Shared Facilities Task Force chaired by Mark Lutter, Duke Energy. Mark has previously volunteered to present this information. Can a CFR be applied to specific pieces of equipment and specific NERC requirements? Nothing entities have seen indicates that it can be applied on a piece by piece and/or requirement by requirement basis. What needs to be in a MOU to adequately demonstrate this?	
APS	The CIP Version 5 Standards do not appear to address the FERC Order 706, paragraphs 473 thru 476, Pg. 126 and 127 (see below). If there is an explicit place where the Standards have addressed this directive, please explain in the response. 473. The Commission adopts its proposals in the CIP NOPR with a clarification. As a general matter, all joint owners of a critical cyber asset are responsible to protect that asset under the CIP Reliability Standards. The owners of joint use facilities which have been designated as critical cyber assets are responsible to see that contractual obligations include provisions that allow the responsible entity to comply with the CIP Reliability Standards. This is similar to a responsible entity's obligations regarding vendors with access to critical cyber assets. 474. Regarding Northern Indiana's comments, we do not believe that this Requirement obligates one joint owner of a critical cyber asset to perform risk assessments of another owner's personnel. Each such owner is responsible for performing assessments of its own personnel. 475. The ERO should consider the suggestions raised by Northern Indiana, SPP and NRECA in the Reliability Standards development process. 476. Therefore, we direct the ERO to modify CIP-004-1, and other CIP Reliability Standards as appropriate, through the Reliability Standards development process to address critical cyber assets that are jointly owned or jointly used, consistent with the Commission's determinations above.	

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
ERCOT		ERCOT respectfully submits that NERC reconsider and revise its proposed response as it appears to conflict with guidance issued regarding control center functionality.
Dominion		Comment: The phrase “there will need to be an agreement” implies an additional requirement. Proposed Change: We recommend removing the first sentence and adding a reference to CIP-002-5.1 prior to “Guidelines and Technical Basis” so that it is clear which standard is being references.
55	What are the complete requirements for BES Cyber Systems without routable or dial-up access?	Refer to the applicability section of each standard.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF recommends that the question and answer here be removed if an answer is not going to be provided.
EEI		Applicability drills down to the sub-requirement level. We recommend changing the answer to: “Refer to the applicability section of each standard and the Applicable Systems column listed in the requirement tables.”
ACES		Why is posting this question and generic answer worthy of a FAQ? An applicability matrix would benefit the industry as a whole. The issue from the question is not where it is written, the problem is that applicability per requirement is not easy to search or filter by from separate .pdfs.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		Yes, this technically answers the question, but adds no value. Seminole suggests that NERC publish a filterable grid on its web site and refer to that grid. This is not difficult to do and adds significant value to entities. NERC has already collected all of the data (transition plan document). Now make it user friendly. If it is frequently asked, address the communications issue.
Duke Energy		Duke Energy suggests removing the above question and answer form the FAQ document. The above provides minimal guidance to the industry.
58	Should entities who receive an XML feed from [their ISO/RTO] as a backup to their ICCP (BES Cyber Asset) consider that as an in-scope resource for CIP Version 5? Is that part of a Medium Impact BES Cyber System?	Redundancy is not an exclusionary consideration in identifying BES Cyber Assets and by extension BES Cyber Systems. If the Cyber Asset, including backup XML feeds, has an impact on the BES, consistent with the definition of a BES Cyber Asset, then it must be classified and protected as a BES Cyber Asset regardless of other Cyber Assets that perform the same function as this Cyber Asset. Each system should be considered separately for its impact on the BES, including backup/redundant systems.
Organization		**Comments**
EEI		This question and answer is unclear. The use of resource is confusing – are they asking about the XML feed or the Cyber Asset that sends or receives the XML feed? We think it's the Cyber Asset that receives the XML feed. Based on this understanding, we recommend revising the answer to: "Responsible Entities should evaluate whether the Cyber Asset that receives the XML feed falls within scope for CIP Version 5. Redundancy does not exclude assets from identification as a BES Cyber Asset or BES Cyber System. The Cyber Asset is in scope if it meets the BES Cyber Asset definition. If in scope, then the Responsible Entity would use

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		CIP-002-5.1 to categorize it by impact rating (high, medium, or low) to determine the applicability of the cybersecurity requirements. If the Cyber Asset meets the BES Cyber Asset definition and the Medium Impact BES Cyber System impact criteria, then it is a Medium Impact BES Cyber System.” It would also be helpful to clarify the question to better align it with the answer.
ACES		Should add ‘within 15 minutes’ to the answer.(?) We’re unclear about what this means for a BES Cyber Asset (System) that is a backup or secondary system. We understand redundancy is not an exclusionary consideration, but have thought this was meant for when considering whether a primary system is a BES Cyber Asset. For example, in a substation if the primary protective relay is working just fine then the backup protective relay, even if it were unavailable, degraded or misused, would not have an adverse impact on the BES within 15 minutes because the primary relay would be the one working, and thus would not be a BES Cyber Asset. Is the answer saying that backup or secondary systems should be considered to be BES Cyber Assets? We understand that backup Control Centers are specifically listed as needing CIP protection and are not asking about them.
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		This example does not necessarily meet the definition of redundancy (an undefined NERC term). ICCP uses different techniques and equipment than XML. A redundant system is a substitutable (interchangeable) system that performs the same functions as the primary system. The XML system uses different techniques and methods. XML is decoupled from ICCP and therefore provides resilience through robust design as opposed to a coupled replacement due to redundant design.
Duke Energy		Duke Energy suggests adding a reference to the definition of BES Cyber Asset into the answer to this question.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
62	In the event of a CIP Exceptional Circumstance, does an entity have to meet all of the CIP requirements that do not specifically mention CIP Exceptional Circumstance?	Yes. The CIP Exceptional Circumstance is listed in six requirement parts. In the instance of a CIP Exceptional Circumstance, the Registered Entity provides evidence that a CIP Exceptional Circumstance has taken place and the timeframe it temporarily suspended compliance with any of those six specific requirement parts. Unless specifically called out in the requirement part (with the phrase “except during CIP Exceptional Circumstances”), compliance to the CIP version 5 standards and requirements must be maintained.

Organization	Comments
EEI	We recommend deleting: “In the instance of a CIP Exceptional Circumstance, the Registered Entity provides evidence that a CIP Exceptional Circumstance has taken place and the timeframe it temporarily suspended compliance with any of those six specific requirement parts.” This sentence does not answer the question and is adding a requirement that is not included in the standards, which is inappropriate for a guidance document.
AEP	AEP supports EEI comments.
MISO	It should be clarified that an entity may be required to drift from its CIP-011 R1.2 procedure in the event of a CIP Exceptional Circumstance or, at least, that an entity may include specific procedures surrounding a CIP Exceptional Circumstance in its CIP-011 R1.2 procedure. For example, CIP-004 governs access management to BCSI, and allows for a CIP Exceptional Circumstance exception. CIP-011 governs procedures for protecting and handling BCSI, but does not allow for a CIP Exception Circumstance exception. Therefore, it should be articulated that access to BCSI may be controlled in accordance with the requirements of CIP-004, which provides for a CIP Exceptional Circumstance, that CIP-011 does not allow.

Number	Question	Answer
63	Does the standard require separate training for each role, function, or responsibility? "	No, all nine elements have to be covered, but a separate course is not required for each.

Organization	Comments

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
North American Generator Forum (NAGF)		The NAGF recommends that the scope of this particular question and answer be made clear that it is limited to CIP-004-5 only as there are other references to roles, functions and responsibilities in other CIP Standards.
EEI		The answer to this question is in the guidelines and technical basis. The question focuses on roles, functions, or responsibility; however, the existing answer focuses on the nine elements and not the roles, which is confusing. We recommend revising the answer to read: “No, the standard does not require separate training for each role, function, or responsibility. The Responsible Entity has flexibility. Refer to the guidelines and technical basis in the standard for additional guidance.”
AEP		AEP supports EEI comments.
Duke Energy		Duke Energy feels that additional clarity should be provided to the answer above. The answer should ensure that all nine elements may be addressed collectively across all trainings, but that separate courses for each are not required.
64	For revocations and transfers, what is the initiating action or when does the clock start for immediate, 24 hours and next calendar day?	From the CIP-004-5 Guidelines and Technical Basis: “This requirement recognizes that the timing of the termination action may vary depending on the circumstance.” The guideline goes on to specify possible processes associated with termination scenarios. The clock starts on revocation when the entity takes action to terminate according to their process. The 24 hour clock starts on the company-determined termination action for terminations and should be completed within 24 hours. For transfers, the revocation must occur by the end of the next calendar day in which a company decides the individual no longer needs access. Business days are not taken into consideration for this Requirement. Entities should be careful to observe these timeframes even on weekends and holidays. An action to terminate could be the notification to the individual of their termination.

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><th>Organization</th><th colspan="2">Comments</th></tr>
<tr><td>EEI</td><td colspan="2">Mixing CIP-004-5 Requirements R5.1 (termination-access), R5.2 (reassignment/transfer), and R5.3 (termination – storage) into one FAQ is confusing and therefore we recommend adding some language (see below) to help clarify. Also, “immediate” revocation language was not included in the final language of CIP-004-5 R5.1 and therefore should not be included in this FAQ. We recommend the following rewrites:
Q: “For access revocation due to a termination, reassignment, or transfer, what action is required to start the clock and when must the revocation be completed by the Responsible Entity?”
A: “From the CIP-004-5 Guidelines and Technical Basis: “the timing of the termination action may vary depending on the circumstance” and provides possible processes associated with termination scenarios. For example, an action to terminate could be the notification to the individual of their termination. The 24 hour clock for revocation starts when the entity takes action to terminate according to their process. For reassignments or transfers, the entity must establish a date when the individual no longer needs access; revocation must occur by the end of the next calendar day after this entity established date. Business days are not taken into consideration for this Requirement. Entities should be careful to observe these timeframes even on weekends and holidays.</td></tr>
<tr><td>ACES</td><td colspan="2">This is ambiguous. A registered entity may take an initiating action a full 24-hours before termination according to its processes. For example, a termination for cause may require CEO approval at small companies. This approval may occur more than 24-hours in advance. The approval could occur on a late Friday afternoon with the actual termination occurring on Monday because of the need to complete paperwork. If the employer revokes access over the weekend to meet the 24-hour timeframe, it could tip off the employee before they are notified. The 24-hour clock should start upon employee notification.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports EEI comments.</td></tr>
</table>

<table>
<tr><th colspan="4">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th colspan="2">Question</th><th>Answer</th></tr>
<tr><td colspan="2">Seminole Electric Cooperative</td><td colspan="2">Add a New paragraph to make it easier to read
For transfers, the revocation must occur by the end of the next calendar day in which a company decides the individual no longer needs access. Business days are not taken into consideration for this Requirement. Entities should be careful to observe these timeframes even on weekends and holidays. Entities may choose to very specifically define how and when the entity determines that access is no longer needed.</td></tr>
<tr><td>77</td><td colspan="2">Where do tie line meters with dial-up modems fall under CIP V5?</td><td>Applicability under CIP V5 depends on the characteristics of the assets (Transmission substations) where the metering equipment is installed and the operating voltage of the tie line the meter is reporting. Because the data reported by the metering system is used for real-time situational awareness, the Cyber Assets associated with the metering will likely be either medium or low impact BES Cyber Assets/Systems, based upon the application of Impact Rating Criteria 2.4, 2.5, 3.2, and potentially 2.6 and 2.8. Once categorized as medium or low impact, the applicable CIP Standards requirements are determined by the applicability statements in each requirement. Certain requirements will be applicable regardless of how the metering BES Cyber Systems communicate with the Control Center. If the BES Cyber Asset is connected to a routable network, even if the routable network is local only to the substation, an Electronic Security Perimeter and Electronic Access Point is required. If the metering BES Cyber Systems are connected serially, the BES Cyber Systems are not required to reside within an ESP. If the metering BES Cyber Systems are dial-up accessible, authentication of the dial-up connection is required where technically feasible.</td></tr>
<tr><th colspan="2">Organization</th><th colspan="2">Comments</th></tr>
<tr><td colspan="2">EEI</td><td colspan="2">The requirements that apply to tie line meters with dial-up modems may vary. The answer to this question appears to assume that all tie line meters are used for real-time situational awareness, which may not be the case. We recommend changing the second sentence that starts with “because” of the answer to: “if the data reported by a metering system is used for real-time situational awareness, then the Cyber Assets associated with the metering will likely be either be medium or low impact…”</td></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
AEP		AEP supports EEI comments.
Duke Energy		Duke Energy believes the answer above should reference the definition of BES Cyber Asset. We offer the following language for clarification. “Because the data reported by the metering system us used for real-time situational awareness, if a tie-line meter is determined to be a BES Cyber Asset, then the Cyber Assets associated with the metering will likely be either medium or low impact BES Cyber Assets/Systems….”
80	If Part 1.4 (Dial Up Connectivity) applies, what other standards have to be applied to that device? Does it revert back to all Medium Impact standards? Or just this one?	Dial-up connectivity is a specific connection mechanism applied to High and Medium Impact BES Cyber Systems under CIP-005 R1 Part 1.4. All other CIP V5 standards applicable to High and Medium Impact BES Cyber Systems would apply, depending on impact classification of the specific BES Cyber System and a lack of unique criteria on the "Applicable Systems" column to specifically exclude the BES Cyber System.
Organization		**Comments**
EEI		This question and answer is unclear. If this is really a question that is frequently asked, we suggest clarifying both the question and the answer. We believe the question may be getting at what requirements apply to a device that uses dial up connectivity. The answer depends on the impact rating – high, medium, or low and whether the appropriate applicable system is listed for the requirement. For example, authentication is required under CIP-005-5 Requirement R1.4 for high and medium impact BES Cyber Systems with dial-up connectivity and their associated PCA. However, if the device is categorized as a low impact BES Cyber System, then CIP-003-6 would apply and not CIP-005-5.
ERCOT		ERCOT suggests that the proposed response note that the requirements specifically addressing “External Routable Connectivity” would not apply.

<table>
<tr><th colspan="4">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th colspan="2">Question</th><th>Answer</th></tr>
<tr><td>81</td><td colspan="2">Regarding CIP-005-5, page 16 in the Guidelines for R1, what is required of the ESP defined for a standalone network (Medium Impact BCS at a substation that meets CIP-002 Attachment 1 Criterion 2.5 that has no External Routable Protocol)?</td><td>As required under CIP-005-5, R1, Part 1.1, "all applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP." Each of the CIP V5 requirements must be reviewed by the Entity to determine their applicability to a medium impact BES Cyber System. Some of the requirements further qualify the "applicable systems," and others do not, making them applicable to those medium impact BES Cyber Systems without External Routable Protocol. If there is dial-up connectivity to the medium impact BCS, then CIP-005-5, R1, Part 1.4 applies as well. If it's truly standalone (no ERC), then the Entity should document the perimeter to prove the components of the BCS are within the ESP.</td></tr>
<tr><th colspan="2">Organization</th><th colspan="2">Comments</th></tr>
<tr><td colspan="2">EEI</td><td colspan="2">We support this question and answer.</td></tr>
<tr><td colspan="2">AEP</td><td colspan="2">AEP supports the response provided.</td></tr>
<tr><td>82</td><td colspan="2">Regarding CIP-005-5, page 17, 2nd paragraph in the Guidelines for R1, are serial ports exempted from the ESP consideration? Can the serial communications extend beyond the 6 walls of the PSP as long as they are terminated inside another PSP? The example is for a substation with multiple control houses with buried fiber cables between the two houses carrying serial signals.</td><td>No requirements are applicable.</td></tr>
<tr><th colspan="2">Organization</th><th colspan="2">Comments</th></tr>
</table>

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
EEI		We support this question and answer.
ACES		Are serials ports exempted from ESP consideration if they are within an ESP? Are they considered a Cyber Asset only if there is routable connectivity? What if the serial ports connect to an IP serial converter? Replying to the two questions that were specific in their scenarios with 'No requirements are applicable' is not an effective response and leads the entity to have to assume answers to these questions creating more confusion.
AEP		AEP supports the response provided.
Seminole Electric Cooperative		NERC should provide a clearer explanation as to why this is not applicable. If understood, then it would not be an FAQ. No CIP-005-5 requirements are applicable. Non-routable serial communications are not part of an ESP (see definition of ESP). Non-routable communication is not required to pass through an EAP (see definition of Electronic Access Point).
ERCOT		ERCOT suggests that NERC note that requirements in other standards would apply (e.g., CIP-007-5 R1).
83	For a substation with Medium Impact BES Cyber Systems, can the ESP be extended to include two control houses with buried cable between the two? Will this communication require alarms, encryption, or something else to	Entities can determine how they want to define their ESPs. For the CIP-006-6 revisions, entities are required to physically protect cabling that extends outside the Physical Security Perimeter for high impact and medium impact Control Centers. Burying the cables or running continuous conduit can be an approach to restricting physical access. Additionally, applying encryption over the connection is also an approach that can be used. This requirement does not apply to substations.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
	meet the draft CIP-006 requirements for the revisions to CIP-006-5?	

Organization	Comments
EEI	We support this question and answer; however, please refer to our general comment on version numbers.
AEP	AEP supports EEI comments.
Seminole Electric Cooperative	First answer the question and then provide the follow up. Don’t know about transmission but some generation does meet this requirement. This requirement only applies to Control Centers. Only Generation and Transmission assets that meets the definition of a Control Center need to comply with this requirement. Entities can determine how they want to define their ESPs. For the CIP-006-6 revisions, entities are required to physically protect cabling that extends outside the Physical Security Perimeter for high impact and medium impact Control Centers. Burying the cables or running continuous conduit can be an approach to restricting physical access. Additionally, applying encryption over the connection is also an approach that can be used.

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td>ERCOT</td><td colspan="2">ERCOT requests that NERC clarify which requirement this statement refers to, “This requirement does not apply to substations.”</td></tr>
<tr><td>84</td><td>For CIP-005-5 R1 Part 1.1: for a medium impact BCS at a substation that is connected via serial communications to the EMS. Inside the substation control room, there is an HMI with a LAN that communicates inside the substation over IP. The language in the standard says "All applicable Cyber Assets connected to a network via routable protocol shall reside within a defined ESP." Which network does "a network" refer to?</td><td>Without knowing the architecture, the following response indicates the minimum that should be done:
There are two networks defined here: The communications network back to EMS and the substation internal network. Because the internal network is routable, there would be a need to create an ESP (as well as a PSP) around the internal network. The guidelines and technical basis entry states: “All applicable BES Cyber Systems that are connected to a network via a routable protocol must have a defined Electronic Security Perimeter (ESP). Even standalone networks that have no external connectivity to other networks must have a defined ESP.”</td></tr>
<tr><th>Organization</th><th colspan="2">Comments</th></tr>
<tr><td>EEI</td><td colspan="2">We recommend removing this FAQ because the communications architecture of the substation is unclear in the question and therefore the answer may not be accurate and could be misinterpreted. A lessons learned document would be more appropriate if it included specific architecture diagrams.</td></tr>
<tr><td>ACES</td><td colspan="2">The question should be corrected for grammar.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
AEP		AEP supports EEI comments.
APS		Recommend this FAQ be removed. The question as currently written has a high degree of situationally specific specificity and the response is based on assumptions.
ERCOT		ERCOT suggests that the proposed response note that the applicability of the ESP for the routable connectivity would be determined on whether the HMI meets the criteria of a BES Cyber Asset.
86	What are the options for utilizing two or more different physical access controls for High Impact BES Cyber System Physical Security Perimeters?	The Guidelines and Technical Basis for CIP-006-6, R1 states: "The FERC Order No. 706, Paragraph 572, directive discussed utilizing two or more different and complementary physical access controls to provide defense in depth. It does not require two or more Physical Security Perimeters, nor does it exclude the use of layered perimeters. Use of two-factor authentication would be acceptable at the same entry points for a non-layered single perimeter. For example, a sole perimeter's controls could include either a combination of card key and pin code (something you know and something you have), or a card key and biometric scanner (something you have and something you are)..."
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF appreciates the reference to Guidelines to support a response and believe this is valuable.
EEI		We support this question and answer.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
ACES		If the FAQs are using the Guidelines and Technical Basis the complete response should be included. This response has omitted an important detail. Page 125 states regarding two or more different physical access controls, “the SDT notes that in some cases it may not be possible to implement two or more different physical access controls due to physical restrictions and equipment locations. Because of this, the language “Where technically feasible” has been included. As is the case with any technical feasibility language within the standard, meeting the requirement language is the goal. Consider the additional language as a response.
AEP		AEP supports EEI comments.
89	If the same PACS system is used for both high and medium locations, do the protections need to be provided at the high level for all locations (even if the badging station location is a low impact facility)?	The definition of the Physical Access Control Systems (PACS) is "Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers." PACS are also associated with providing protections of BES Cyber Systems. As such, the PACS Cyber Assets have protections that must be applied according to the specific requirements of CIP V5 and should assume the protections required for the highest rated BES Cyber System with which it is associated.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF believes there may be value in explaining that this is the same situation when applied to EACMS. The NAGF also notes that it is confusing if the question is asking about badge readers or other Cyber Assets associated with PACS. A “badging station location” may refer to a badge reader (excluded from being a PACS) or some other Cyber Asset that may actually be in scope and classified as a PACS.
EEI		The last sentence seems to imply that PACS systems associated with high impact BES Cyber Systems (BCS) as an Applicable System must also meet the compliance requirements for high impact BCS where are there are no additional Applicable Systems. Therefore, the last sentence should be changed to read “If the same PACS system is used to control physical access to both high and medium impact BCS, then all of the requirements for high and medium impact BCS that include their associated PACS would apply to that single PACS system. However,

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
		requirements for high and medium impact BCS where PACS is not listed as an associated Applicable System would not apply to that single PACS system.”
ACES		The response should be re-written for clarity. Start with the last sentence as it answers the question. The first part of the paragraph explains the answer.
AEP		Physical Access Control Systems do not all share the same architectures or capabilities. Generally speaking, there are 3 common types of components to a PACS: the servers, workstations, and controllers. Many Physical Access Control Systems are capable of limiting the functionality and scope of their components based on the entity’s specific needs. AEP agrees that a PACS server should be protected based on the highest impact BES Cyber System it is associated with. PACS workstations can serve a variety of purposes in the operations of the PACS and should not be treated equally. A PACS workstation used for system administration has more capabilities than a workstation located at a remote facility. The admin workstation then requires more protections than the remote workstation and should be classified according to the highest impact BES Cyber System the PACS is associated with. A workstation at a remote, may be limited to performing PACS functions for that location, such a workstation should be classified according to the highest impact BES Cyber Systems it performs PACS functions for. A PACS controller would have an association with the highest rated BCS where it is located. A PACS controller or workstation that is not associated with and BCS or capable of providing PACS functions for a BCS, would not be in the CIP program.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
Seminole Electric Cooperative		There are multiple ways to read this response. This answer could be read to require dual/2 factor authentication at all locations if any location protected by the PACS is high impact. Seminole does not believe that it is meant to be read that way. If it is, then NERC has a much bigger issue in how the industry understands the requirement. This should be rewritten into plain English. If the compliance language was truly understood, then the FAQs would not be needed.
APS		The situation in this FAQ appears to be similar to the Pilot Relay question in which NERC has previously stated “associated with” would not require a far end relay at a lower-impact rated location (note: BCS are rated, not locations) to assume a high-watermark treatment. In this FAQ, it is being said that “associated with” requires a high-watermark to be applied for PACS Cyber Assets regardless of location. The sentence that appears to imply this is: “As such, the PACS Cyber Assets have protections that must be applied according to the specific requirements of CIP V5 and should assume the protections required for the highest rated BES Cyber System with which it is associated.” Due to the sensitivity around this issue APS would recommend that the FAQ be reworded for additional clarity to align with previously published NERC guidance.
90	What does the testing requirement in CIP-006-5, R3, Part 3.1 mean for PACS workstations and servers? Does that need to be documented the same way the card readers/door alarms are?	PACS workstations and servers should be tested in such a way to demonstrate "they function properly" as required in Part 3.1. Since these Cyber Assets do not perform the same functions as the card readers/door alarms, the actual testing and documentation may differ. Sufficient evidence should be documented to demonstrate the Cyber Assets were tested and "function properly". One method of accomplishing this would be to: (a) create a set of test scripts for the Cyber Assets (collectively or individually) to demonstrate they are functioning properly, (b) execute them as required, (c) and document the results of the executed tests. PACS workstations functional tests include, but may not be limited to, granting, revoking, monitoring, and logging of access.
Organization		**Comments**

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td colspan="2">North American Generator Forum (NAGF)</td><td>The NAGF recommends changing the 2nd paragraph to read, “PACS workstations functional tests “may” include, but may not be limited to…” to show that these are examples of functional tests but not mandated by the language within the Standard.</td></tr>
<tr><td colspan="2">EEI</td><td>The definition of PACS is “Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter such as motion sensors, electronic lock control mechanisms, and badge readers”; however, the answer to this question refers to “granting, revoking, monitoring.” To be consistent with the PACS definition, we recommend editing the last sentence of the answer to read: “PACS workstations functional tests include controlling, alerting, or logging access.”</td></tr>
<tr><td colspan="2">AEP</td><td>AEP supports EEI comments.</td></tr>
<tr><td colspan="2">Seminole Electric Cooperative</td><td>Does successful real-time use of a system to grant, revoke, monitor, and log access demonstrate a successful test? If so, then say so with guidance.

PACS workstations functional tests include, but may not be limited to, granting, revoking, monitoring, and logging of access. A successful test demonstrates the task was performed correctly. A test may consist of verification of successful completion of normal operations.

If this does not meet the requirements, then say so as that is how we currently intend to demonstrate testing as part of our normal periodic review process.</td></tr>
<tr><td colspan="2">ERCOT</td><td>ERCOT suggests that the proposed response note that CIP-009-5 recovery testing may be an approach to demonstrate compliance with this requirement related to the PACS.</td></tr>
<tr><td colspan="2">Duke Energy</td><td>Duke Energy suggests adding the word “may” in the following sentence, “PACS workstations functional tests may include, but may not be limited to, granting, revoking, monitoring, and logging of access. We believe not adding the word “may” in this sentence expands the scope of CIP-006-5, R3, Part 3.1</td></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		Not all PACS workstations are in scope?
91	"(M)onitor…for unauthorized physical access" for the individual devices that make up the PACS system. Or is this directed to the servers that host the PACS? Do you need to alarm/alert on each of the guard and badging workstations?	Yes, the physical access to the PACS servers, controllers, and guard and badging systems is monitored and alerted on for potential unauthorized access. In accordance with CIP-006-6, R1, Part 1.6, all devices that make up the PACS system including servers, controllers, and workstations should be brought into scope for this requirement.

Organization	Comments
North American Generator Forum (NAGF)	The NAGF recommends removing the word "all" from the 2nd sentence to clarify that it does not include those items specifically excluded from being PACS (i.e. badge readers, door hardware, etc.).
EEI	It is our understanding that this question was rewritten to remove references to the study participants; however, now it is unclear. We recommend the following rewrites to the question and answer to help clarify. Q: "Is CIP-006-5 R1.6 and R1.7 intended to including monitoring and alerting on guard and badging workstations?" A: "The obligations for an entity for CIP-006-5 R1.6 and R1.7 depend on the configuration of the PACS. If an entity considers the workstations to be PACS associated with high impact BES Cyber Systems or medium impact BES Cyber Systems with ERC, then monitoring is required under R1.6 and alerting is required under R1.7. Some guard and badging workstations may not be considered PACS by an entity, depending on the configuration, and, therefore, monitoring and alerting would not be required for the workstations not considered PACS."

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
ACES		For CIP-006-6m R1, Part 1.6 (and Part 1.7), the NERC response seems to imply that each PACS has its own monitoring system. If the devices that make up the PACS are all within a PSP, and the entity has authorized everyone that has authorized unescorted access into that PSP to have access to all the Cyber Assets within the PSP, then the monitoring and alerting of unauthorized access into the PSP seems to meet Part 1.6 (and Part 1.7) and no additional PACS specific monitoring and alerting are required. Can NERC confirm this interpretation?
AEP		AEP supports EEI comments.
Duke Energy		Duke Energy suggests removing the word "all" in the following sentence, "In accordance with CIP-006-6, R1, Part 1.6, all devices that make up the PACS system including servers, controllers, and workstations should be brought into scope for this requirement. " because not all devices should be in scope.
92	What are examples entities may use when inventorying all known enabled default or generic account types?	Some of the ways to identify default and/or generic accounts include: • Vendor provided lists of the required accounts on a system. • Tools that can be run to identify user accounts created on a local system (e.g., Nessus Credential Scans). • Tools such as AD (or LDAP Queries) may have a listing of accounts with access to systems. • Review the device/application web sites or support to identify if there are default accounts.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF recommends caution in not calling out a particular technology (Nessus, AD, etc.) especially in light of the response to FAQ #93.

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td>EEI</td><td colspan="2">We support this question and answer.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports the response provided.</td></tr>
<tr><td>Seminole Electric Cooperative</td><td colspan="2">Yes. But does not answer the question. If not willing to answer the question (and likely shouldn’t), then make a statement such as:
NERC cannot provide a recommended list to entities as there are significant differences in the equipment in use across the sector. Some of that an entity may identified their default accounts include:…</td></tr>
<tr><td>93</td><td>Are password safes recommended?</td><td>A password safe is a utility application that is used to securely store a set of passwords and pass phrases. While the ERO Enterprise (NERC and the Regional Entities) cannot recommend or endorse the use of any particular technology, password safes can be an effective tool in an organization’s overall cybersecurity program when used properly, and their use should adhere to the entity’s CIP-011 Information Protection program.</td></tr>
<tr><th>Organization</th><th colspan="2">Comments</th></tr>
<tr><td>EEI</td><td colspan="2">We support this question and answer.</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports the response provided.</td></tr>
<tr><td>APS</td><td colspan="2">Although the intention is not to endorse a solution, this FAQ may encourage the use of a password safe. This is arguably a good or bad security idea depending on the organization’s risk profile. Consider removing this FAQ.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
ERCOT		ERCOT suggests that the response provide additional clarification regarding when a password safe would be subject to an entity's CIP-011 program, e.g., when the password safe contains information subject to such program.
94	Signage for physical port protection (CIP-007-5, R1.2) – is it acceptable to place signs at the PSP doors, rather than on each individual device port?	Signage is explicitly allowed as a measure of compliance. If signage is used, the sign (in the appropriate language for the Responsible Entity) must be as close to the applicable port as possible to be effective to deter inappropriate use of the port.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF recommends rewording the answer to both allow for signage and to leave it up to the entities to determine the most effective place for the signage as the proximity to the applicable port is not mandated by the Standard.
EEI		The second sentence in the response is awkward and appears to expand or interpret the language of the standard, "as close…as possible" in particular. As close as possible may be interpreted as on top of or on, which suggests that tamper tape is the only option. To address this concern, we recommend editing the language of the second sentence in the response to: "If a sign is used, then its placement and the language used on the sign are both considerations for determining whether it conveys that the port should not be used without proper authorization." Also, we recommend adding the following language to the answer, including filling in the appropriate dates marked by Xs: "In addition, the requirement does not require demonstrating that a protected, physical input/output port that is unnecessary for network connectivity, console commands, or removable media has not been used. For more details, refer to the measures column, the guidelines and technical basis, and violation severity level in the standard for this requirement. For example, the guidelines and technical basis for the requirement states: "this control, with its inclusion of means such as signage, is not meant to be a preventative control against intruders…signage would be used to remind authorized users to "think before you plug anything into one of these systems which is the intent.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		(NOTE: this FAQ replaces a draft lesson learned guidance that was posted on the NERC CIP V5 implementation webpage from XXX, 2014 to XXX, 2015.)”
ACES		So the answer about signage on the PSP doors is “No”?
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		Possibly add a statement at the end. While some entities may choose to use signage to demonstrate compliance, entities may still choose to utilize other technical controls where available. I have also heard that this may result in a recommendation or area of concern that is not a violation. If accurate, then say so. It should not fall on the Entity to make a compliant decision and then later receive a recommendation/area of concern from its Regional Entity that it is compliant, but substandard.
ERCOT		ERCOT requests that NERC clarify where this is required and how close is “as close as possible to be effective…” Would signage at the door not be sufficient to cover all equipment within the PSP?
Dominion		Comment: The language in the FAQ includes the word “must” and exceeds the language in the standards. The response should be reworded. Proposed Change: Reword as: Signage is explicitly allowed as a measure of compliance. If signage is used, consideration should be made to ensure the sign is visible to be an effective deterrent to an inappropriate use of the port.
Duke Energy		Duke Energy does not agree with the response provided. While a sign is an acceptable means and is allowed per the standard, location and proximity is not. It should be up to the Responsible Entity to ultimately decide the proper

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		location of a sign. Safety considerations is just one example that could inhibit an entity from placing signs at each PSP door or individual port.
98	For CIP-007-5 R3 Part 3.1 on malicious code for non-routable sites, is hardening or group policy sufficient?	“System hardening," "policies," etc. have been provided as examples of acceptable measures of meeting the requirement to "deploy method(s) to deter, detect, or prevent malicious code". While these methods are defined as acceptable, they should be documented in such a way to demonstrate their applicability to the desired BES Cyber Systems and their ability to provide the required control.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF recommends that clarity be added to the response that this is applicable to all high and medium impact BES Cyber Systems, not just non-routable ones. The NAGF would also like clarity to be provided on what guidance can be provided for “hardening” techniques.
EEI		The use of “while” to start off the second sentence of the response suggests that these methods are defined as acceptable but may not really be acceptable, which is confusing. We recommend rewording the second sentence to: “these methods are defined as acceptable, if documented to demonstrate their applicability to the desired BES Cyber Systems and ability to provide the required control.”
AEP		AEP supports EEI comments.
Dominion		Comment: The use of “while” to start off the second sentence of the response suggests that these methods are defined as acceptable but may not really be acceptable, which is confusing. Proposed Change: We recommend rewording the second sentence to: “These methods are defined as acceptable, if documented to demonstrate their applicability to the desired BES Cyber Systems and ability to provide the required control.”

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
101	How should an entity treat the devices that do not have accounts but use separate passwords to delineate the role of the user? (substations). What about situations where there are no accounts, only passwords, but the users don't have access to the passwords?	Devices that utilize passwords without an associated user ID must be included in the registered entity's inventory of default and generic accounts. In these cases, a null account name may be used. It may be advisable to include a field in the inventory where additional identifying details can be associated with the null account name, such as a brief description of the user role associated with that password. For those BES Cyber Assets identified in the applicable systems column, access to a Cyber Asset with only a password should be considered a "generic account type," and individuals who have authorized access to these shared type of accounts should be documented as such. Entities are not expected to document the passwords themselves for these "generic account types." Caution: Evaluate if these are default passwords.

Organization	Comments
North American Generator Forum (NAGF)	The NAGF is unsure what the 2nd question is asking (is this a service account? interactive user account with no users? etc.). The answer provided doesn't seem to provide a specific response to the 2nd question.
EEI	To tie the response to the language of the standard and remove "must" from the first sentence of the response, we recommend rewording the first sentence to: "include devices that utilize passwords without an associated user ID in the CIP-007-5 R5.2 inventory of known enabled default or other generic account types." In the third sentence of the response, remove "in the applicable systems column" and add "as being accessed by such a password" to remove the implication that a spreadsheet or database table is the specific inventory method. The edited sentence should be: "For those BES Cyber Assets identified as being accessed by such a password, access to a Cyber Asset with only a password…."
AEP	AEP supports EEI comments.

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td>Seminole Electric Cooperative</td><td colspan="2">Cut to the chase in the answer. Seminole understands that NERC cannot name Cisco (and their competition), but NERC can and should imply it. Otherwise, entities will not pick up on this.

Devices, including some networking hardware, that utilize passwords without an associated user ID must be included in the registered entity’s inventory of default and generic accounts…</td></tr>
<tr><td>Dominion</td><td colspan="2">Comment:
To tie the response to the language of the standard and remove “must” from the first sentence of the response.

Proposed Change:
We recommend rewording the first sentence to: “Include devices that utilize passwords without an associated user ID in the CIP-007-6 R5.2 inventory of known enabled default or other generic account types.” In the third sentence of the response, remove “in the applicable systems column” and add “as being accessed by such a password” to remove the implication that a spreadsheet or database table is the specific inventory method. The edited sentence should be: “For those BES Cyber Assets identified as being accessed by such a password, access to a Cyber Asset with only a password….”</td></tr>
<tr><td>107</td><td>Question 1: What level of testing should be done to develop baselines?

Question 2: Are entities expected to perform a penetration test for CIP-010? If so, what is the appropriate scope?</td><td>Response 1: Testing (e.g., penetration testing) is not specifically required to develop a baseline, but all five parts of CIP-010-1, R1, Part 1.1 must be a part of the baseline. In some cases automated tools may be necessary to develop the baseline, for example logical ports identification as a part of the baseline and in accordance with CIP-007-5, R1, Part 1.1.

Response 2: Penetration testing is not required for CIP-010, but an active vulnerability assessment is an option under CIP-010-1, R3, Part 3.1, and a requirement under CIP-010-1, R3, Part 3.2. An active vulnerability assessment is described in the Guidelines and Technical Basis section of CIP-010-1, R3.

For a discussion on a similar topic, see also FAQ #111.</td></tr>
<tr><th>Organization</th><th colspan="2">Comments</th></tr>
</table>

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
EEI		We recommend splitting the two questions into two separate questions since this is the only FAQ with two questions. We also recommend avoiding the cross reference to another FAQ, especially if the ID number will be dropped or changed in the final FAQ supporting document.
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		Remove the FAQ number Note: The “number” column in the table below is not relevant to stakeholders and is only included as an organizational tool for NERC.
ERCOT		ERCOT suggests that proposed response 1 is not fully responsive to the question, e.g., penetration testing is not contemplated in the definition of a baseline. Additional clarification regarding the types and scope of testing NERC believes is necessary to develop the baseline initially would be helpful. ERCOT also suggests that proposed response 2 note that, while not required, the use of a penetration test is at the discretion of the entity. Finally, ERCOT notes that FAQ 111 is not included in this document for appropriate review of supporting material.
Dominion		Comment: We support EEI’s comment for this response. Proposed Change: Recommendation: split the two questions into two separate questions since this is the only FAQ with two questions. We also recommend avoiding the cross reference to another FAQ, especially if the ID number will be dropped or changed in the final FAQ supporting document.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
108	How should active vulnerability scans be managed for PACS systems given their sensitivity to Denial of Service?	CIP-010, R3.1 gives responsible entities the option to conduct a paper or active vulnerability assessment. Accordingly, the responsible entity should choose the option that will yield the optimal results given its PACS susceptibility to Denial of Service attacks. For instances, if the PACS is highly susceptible to Denial of Service attacks, then the entity should only conduct paper vulnerability assessments. Although an active vulnerability assessment is required every three years for a high impact BES Cyber System, this does not apply to PACS.

Organization	Comments
EEI	We support this question and answer.
AEP	AEP supports the response provided.
Seminole Electric Cooperative	For completeness and easier reading, add something like …For instances, if the PACS is highly susceptible to Denial of Service attacks, then the entity should only conduct paper vulnerability assessments. (New paragraph) An active vulnerability assessment is required every three years for a high impact BES Cyber System, this does not apply to PACS. An active vulnerability assessment is required prior to adding a new high impact BES Cyber Asset, EACMS, or PCA. However, this requirement does not apply to PACS.
APS	Suggest the question be reworded so it is more broadly applicable. For example, “How should active vulnerability assessments be managed for environments that are sensitive to Denial of Service or other negative impacts?” This would require a modification to the response as well to remove the references to PACS.

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
		If a Cyber Asset is susceptible to Denial of Service or other negative impact, it should be logged as a vulnerability and either be remediated or mitigated in accordance to CIP-010-1 R3, part 3.4.
128	For v3 Critical Assets and associated Critical Cyber Assets that will be classified as low impact BES Cyber Systems under v5, what is expected for declassification and destruction of critical information if the facility remains in operation?	If the information is specific to the asset, then information pertaining to that asset is also declassified and will be subject only to the entity's normal information security policies. If the information on the declassified asset includes information on other assets that will not be declassified, the information will need to be treated as BES Cyber System Information.

Organization	Comments
EEI	If a v3 Critical Cyber Asset becomes a Low Impact BES Cyber System under v5, then CIP-011-1 no longer applies to that asset and therefore the information on the declassified asset is not subject (applicable) to CIP-011-1. To clarify this in the response, we recommend revising the answer to: “CIP-003-5 and CIP-011-1 do not require BES Cyber System Information associated with Low impact BES Cyber System to be protected. When a cyber asset identified as a Critical Cyber Asset under Version 3 is classified for the purpose of CIP Version 5 as a Low impact BES Cyber System, the applicable CIP-003-3 requirements no longer apply and therefore there is no obligation to declassify or destroy the information.”
ACES	Wouldn’t the registered entity follow their own BES Cyber System Plan as per “CIP-011-1 R2, “Each Responsible Entity shall implement one or more documented processes that collectively include the applicable items in CIP-011-5 Table R2 – Media Reuse and Disposal.” Information as to how and when to remove or declassify information should be in that plan. As per page 176 from the SDT industry comments response, “Some commenters were confused about which requirements applied to Low Impact BES Cyber Systems. CIP-011 does not apply to Low Impact systems. The drafting

<table>
<tr><th colspan="3">Specific Comments – April 1, 2015 Posting</th></tr>
<tr><th>Number</th><th>Question</th><th>Answer</th></tr>
<tr><td></td><td colspan="2">team moved all requirements that apply to Low Impact systems into CIP-003-5.” Does the answer given here conflict with this statement,” If the information on the declassified asset includes information on other assets that will not be declassified, the information will need to be treated as BES Cyber System Information.”?</td></tr>
<tr><td>AEP</td><td colspan="2">AEP supports EEI comments.</td></tr>
<tr><td>Seminole Electric Cooperative</td><td colspan="2">Seminole suggests that this be rewritten for clarification. Classified is used three different ways in this FAQ and response; protected information, categorization of the system, and reassignment of system category.
Change the question to use the term categorized, the term used in the title of CIP-002. This avoids potential misapplication of the word declassification.

For v3 Critical Assets and associated Critical Cyber Assets that will be categorized as low impact BES Cyber Systems under v5, what is expected for declassification and destruction of critical information if the facility remains in operation?

The asset is not being declassified – it is a Critical Asset that will be categorized as low impact with reduced information protection requirements. No suggested rewording.
…If the information on the declassified asset includes information on other assets…</td></tr>
<tr><td>APS</td><td colspan="2">This response assumes that all entities have “normal” information security policies (e.g., non-CIP related) which may not be accurate. The response should state, very clearly, what is required in this situation. It is our understanding that there are no requirements for information protection for any low-impact BCS. Therefore, the answer would simply be “No requirements are applicable”.</td></tr>
<tr><td>ERCOT</td><td colspan="2">ERCOT suggests that NERC’s proposed response include information regarding retention of evidence for audits that might span v3 and v5.</td></tr>
</table>

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
Dominion		Comment: If a v3 Critical Cyber Asset becomes a Low Impact BES Cyber System under v5, then CIP-011-2 no longer applies to that asset and therefore the information on the declassified asset is not subject (applicable) to CIP-011-2. Proposed Change: To clarify this in the response, we recommend revising the answer to: "CIP-003-5 and CIP-011-2 do not require BES Cyber System Information associated with Low impact BES Cyber System to be protected. When a cyber asset identified as a Critical Cyber Asset under Version 3 is classified for the purpose of CIP Version 5 as a Low impact BES Cyber System, the applicable CIP-003-3 requirements no longer apply and therefore there is no obligation to declassify or destroy the information."
129	For a BES Cyber Asset in a medium impact facility, if the device breaks and has to be sent to a vendor, what does an entity need to do to ensure the integrity of the information on that device is protected as required by the standard?	CIP-011 does not explicitly address the case where a device must be sent to a vendor. However, in such a case when the device in question is presumably being sent to the vendor for redeployment or disposal, the responsible entity would have to comply with the requirements of R2.1, which address the reuse of Cyber Assets. If the device is not released for reuse or is not being disposed, the entity should either retain or wipe the BES Cyber System Information or the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2. Responsible Entities should keep in mind that not all data requires protection under the CIP standards. Responsible Entities should evaluate whether the Cyber Asset contains any data that should be classified as BES Cyber System Information or any critical energy infrastructure information (CEII) and protect the information accordingly.
Organization		**Comments**
North American Generator Forum (NAGF)		The NAGF recommends to expand the response for not only a device that breaks, but a device that needs to be sent to a vendor or any 3rd party around other scenarios (troubleshooting, maintenance, incident response, etc.). The same answer should apply to these circumstances.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
EEI		The last sentence of the answer pulls in a term that is not included in CIP-011 or defined by NERC: critical energy infrastructure information (CEII). We recommend the following rewrite of this sentence to fix this issue and help align the response with the standard: “Responsible Entities use their CIP-011-1 R1 documented information protection program to identify and protect BES Cyber System Information.”
ACES		There is no R2.1. We presume you mean Part 2.1. The answers should use correctly terminology when referring to the standards.
AEP		AEP supports EEI comments.
Seminole Electric Cooperative		Good point on CEII. However, CEII should be addressed in a separate sentence to make clear that this is an additional recommendation not subject to CIP. Most CEII information does not meet the definition of BES Cyber System Information. Definition: “Information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System.” Responsible Entities should keep in mind that not all data requires protection under the CIP standards. Responsible Entities should evaluate whether the Cyber Asset contains any data that should be classified as BES Cyber System Information and protect the information accordingly. Additionally, it is suggested that Responsible Entities consider whether any critical energy infrastructure information (CEII) data is included and protect the information accordingly.
APS		Recommend removing CEII as that is not relevant to the CIP Standards. The definition of BES Cyber System Information (BCSI) does not make reference to this specific type of information. This response does not address the access control elements from CIP-004-5 that may need to be followed by a vendor. It also does not address potential other information protection requirements that may have been

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
	established by each Responsible Entity's Information Protection Plan. This could include various third-party contractual obligations that need to be explored on a case-by-case basis. It should be noted, that the requirements do not specifically state that a chain of custody practice must be adopted nor is there an explicit requirement to keep BCSI within a physical security perimeter. There may be many other ways to securely "handle" the BCSI.	
ERCOT	ERCOT suggests that the proposed response is not fully responsive to the question. The question seems to be referencing situations where a device fails (broken) to a point that the entity can do nothing to dispose of the data and/or cannot clear the data from the device prior to sending it off-site. The proposed response should also include guidance regarding what the compliance obligations are in that scenario.	
Dominion	Comment: 1st paragraph, there is no requirement in the standard to document custodial care for media in transit. If the device is not released for reuse or is not being disposed, the entity should either retain or wipe the BES Cyber System Information or the Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter prior to actions taken by the entity as required in R2. The last sentence of the answer pulls in a term that is not included in CIP-011 or defined by NERC: critical energy infrastructure information (CEII). Proposed Change: Remove phase: Responsible Entity should maintain documentation that identifies the custodian for the data storage media while the data storage media is outside of the Physical Security Perimeter. We recommend the following rewrite of the last sentence to fix this issue and help align the response with the standard: "Responsible Entities use their CIP-011-2 R1 documented information protection program to identify and protect BES Cyber System Information."	

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
Duke Energy		Duke Energy suggests removing the reference to CEII as it is not an enforceable standard.
130	For destruction of data what would be considered a minimum standard to ensure data is destroyed? (Degausser and hydraulic crusher)	The requirement is that the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. The Responsible Entity should ensure that the media containing BES Cyber System information cannot be retrieved in any way. Procedures should be tested to ensure that the method(s) used achieves the goal of destruction. Degaussing and crushing are two of many ways to destroy media. Other methods include, but are not limited to, multi-pass wiping, drilling of platters, shredding, etc. In some cases, two or more methods could be used to ensure data destruction. The Guidelines and Technical Basis offer suggestions on how the destruction can be performed, including information from NIST SP800-88.

Organization	Comments
North American Generator Forum (NAGF)	The NAGF recommends removing the sentence, "Procedures should be tested to ensure that the method(s) used achieves the goal of destruction". This expands the requirements within the Standard. Verification of wiped media is not part of the Standard and is not readily available to most entities. The entity has the flexibility to determine the appropriate level and approved methods.
EEI	We recommend removing the sentence "the Responsible Entity should ensure that the media containing BES Cyber System information cannot be retrieved in any way" and the following sentence that requires testing of destruction procedures because they modify and add requirements to CIP-011-1 R2.2. The destroy option in CIP-011-1 R2.2 is to destroy the data storage media and not the data. The standard does not require Responsible Entities to ensure that the information on the media cannot be retrieved in any way nor does it require Responsible Entities to test its destruction procedures to validate that the information cannot be retrieved. Acceptable evidence includes "records that indicate that data storage media was destroyed" and does not mention ensuring that the information cannot be retrieved in any way or testing procedures to verify that the information cannot be retrieved.

Specific Comments – April 1, 2015 Posting		
Number	**Question**	**Answer**
	The Guidelines and Technical Basis for CIP-011-1 explains that “if the media is to be reused outside of a BES Cyber System or disposed of, the entity must take action to prevent the unauthorized retrieval of BES Cyber System Information from the media…. Media sanitization is the process used to remove information from system media such that reasonable assurance exists that the information cannot be retrieved or reconstructed.” Reasonable assurance does not mean ensuring that the information cannot be retrieved in any way nor does it require testing the procedure to make sure it cannot be retrieved in any way. The Guidelines and Technical Basis also explain that “clearing techniques may provide a suitable method of sanitization for media that is to be reused, whereas purging techniques may be more appropriate for media that is ready for disposal.” The Guidelines and Technical Basis also points to NIST SP800-88 for additional guidance on the types of actions that an entity could take to “prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.” This gives entities flexibility to choose the appropriate method to prevent the unauthorized retrieval of BES Cyber System Information. This is further supported by the Order 706 SDT in its Consideration of Comments: “The method that an entity chooses to implement to meet these requirements is left to the discretion of the entity…the entity may not be able to present evidence that they have ‘prevented’ any and all unauthorized retrieval.” Also, specific to the destroy option, the SDT states “destruction is only needed in the event that unauthorized retrieval cannot be prevented. (NERC Consideration of Comments, Cybersecurity Order 706 Version 5 CIP Standards, p 177-78, available at: http://www.nerc.com/pa/Stand/Project20086CyberSecurityOrder706Version5CIPStanda/C_of_C_Project2008-06_CIPv5_20120412_Final.pdf). We support the rest of the response because it appears to align with the language of the requirement and the Guidelines and Technical Basis of the requirement.	
AEP	AEP supports EEI comments.	

Specific Comments – April 1, 2015 Posting

Number	Question	Answer
Dominion		Comment: Dominion is in support of EEI comments for this response. Proposed Change: We recommend removing the sentence "the Responsible Entity should ensure that the media containing BES Cyber System information cannot be retrieved in any way" and the following sentence that requires testing of destruction procedures because they modify and add requirements to CIP-011-2 R2.2.
Duke Energy		Duke Energy suggests removing the following sentence, "Procedures should be tested to ensure that the method(s) used achieves the goal of destruction." because having procedures and methods to test and ensure destruction of data is not part of the NERC standard.