Individual or group. (34 Responses)
Name (23 Responses)
Organization (23 Responses)
Group Name (11 Responses)
Lead Contact (11 Responses)
IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE. (1 Responses)
Comments (34 Responses)
Question 1 (33 Responses)
Question 1 Comments (33 Responses)
Question 2 (33 Responses)
Question 2 Comments (33 Responses)
Question 3 (33 Responses)
Question 3 Comments (33 Responses)

Group
Dominion
Connie Lowe
Yes
No
No
Group
Colorado Springs Utilities
Shannon Fair
Yes
No
Yes
Identify, Assess, and Correct Compliance Language - We think the ‘identify, assess, and correct’ language is adequate if NERC defines what the minimum criteria is for each program being implemented. Requirements for Low Impact BES Cyber Systems - We think there should be guidance that establishes a baseline of minimum expectations for the four topic

areas, along with a definition of the minimum auditable documentation required to demonstrate compliance. 30-Day Exemption or exemption of transient devices from compliance with the standards - A 30 day exception could allow insecure devices to be introduced to the ESP. The definition of BES Cyber Asset should be extended to cover these types of devices. For example, transient systems could be defined as a specific type of Cyber Asset (perhaps as a Maintenance Cyber Asset or a Transient Cyber Asset) along with guidance on minimal security expectations for the new type of Cyber Asset. Survey of BES Cyber Assets that do not satisfy the"15-minute" parameter described in the Guidelines of CIP-002-5 - Any standard needs to clearly define how the 15-minute parameter should be applied. For example, is the 15 minutes applicable to normal operations, intentional misuse, or device failure?
Group
SRC
Greg Campoli
SRC, supported by CAISO, ERCOT, IESO, MISO, & PJM
Yes
No
Yes
CIP Version 5 is an important step forward for the electric subsector to continue to demonstrate leadership in the development of policy and regulations for securing critical infrastructure. The FERC Order 791 gives NERC a year to respond to significant items the commission identified. The SRC believes that establishing a Standard Drafting Team (SDT) to respond to the commission order is appropriate and necessary. It is important to note that adequate time should be provided to enable the SDT to assess and adopt the effective solutions to meet the items the commission is seeking. Depending on NERC's response to Order 791, the implementation timeline could be impacted, especially if the changes or guidance included in the response have significant impact on the implementation efforts. The RAI project is a multi-year initiative that NERC is currently pilot- testing to improve the compliance monitoring and audit process. The IRC believes RAI is a positive and promising approach but it needs to be vetted through the pilots and will not be ready for general-availability until 2015. NERC's proposal to use ES-C2M2 framework as a benchmark for CIP standards will require further evaluation and analysis before this can be understood and applied as a potential measurement solution linked to the NERC CIP standards. Before adopting ES-C2M2, NERC and the industry need to monitor and understand how CIP, RAI and ES-C2M2 would be integrated. If not addressed appropriately, incorporating the ES-C2M2 framework could drive significant scope expansion impacting both audits and ISO operational requirements. RAI is a voluntary program and the prototypes are scheduled for two more years making it difficult to link to the FERC one year requirement. Additionally RAI has not been tested in CIP at this time. ES-C2M2 is an enterprise risk program and audit

scope and standards links with CIP are unclear. There are concerns how RAI and ES-C2M2 fit into NERC scope as a solution. The SRC believes NERC should focus on RAI for now and incorporate ES-C2M2 at a later time. As it is, the RAI timeline is two years out. If ES-C2M2 is also bundled in, the industry will have to wait even longer. Incremental improvements are far easier and provide the flexibility to adapt to emerging risks and threats, rather than complete make-over's. The SRC agrees that the 'Indentify, Assess and Correct' (IAC) approach can be removed from the CIP Standards, while still avoiding a 'zero defect/tolerance' approach to standards enforcement. The Standards Drafting Team should work on developing a clear alternative that is acceptable to the industry, the regional entities, NERC and to FERC. SAR, Page3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices. Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. The Standard Drafting Team should consider a tiered approach when defining communication networks and standards to protect those elements. It doesn't have to be a one-size-fits-all. This is especially important for Physical protections. The SRC is committed to helping NERC respond to the commission's issues and will continue to provide support to the CIP Version 5 drafting team and RAI project initiatives.

Group

Northeast Power Corodinating Council

Guy Zito

No

: Recommend modifications to the SAR language to clarify and align with FERC order 791:SAR, page 3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."• Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices.• Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. NPCC recommends the following be considered: i) Suggest changing the

Detailed Description's second bullet to The SDT shall consider the development of necessary Standard modification or new Standards that address security controls for Low Impact assets. ii) Suggest splitting the Detailed Description's third bullet into two bullets for clarity. Replace this third bullet with the following a - c. a) The SDT shall consider how to define the term transient device. b) The SDT shall consider whether further Standard protections are needed to address vulnerabilities associated with transient devices. c) The SDT will review the results of the ERO survey concerning the use of the "15 minute" parameter to inform the SDT's development of a new / modified Standards for the protection of Cyber Assets and BES Cyber Systems from the vulnerability introduced by transient devices.
No
Yes
NERC staff requested that the industry not submit Requests for Interpretation (RFI). However, more detailed reviews of the approved CIP Version 5 Standards generated additional questions regarding com,pliance. NPCC members are requesting a process for seeking clarifications so that company implementation expectations of CIP Version 5 will be consistent with future audit expectations. Recommend removing the “identify, assess, and correct” language in 17 CIP Version 5 requirements. Recommend that the Standard Drafting Team develop a new standard that will allow allow this one standard to have an implementation date later than the other Version 5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. Recommend drafting a definition based on impact to BES for transient devices and categories for device types. Recommend that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Recommend that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards.
Individual
Antonio Richmond
CPS Energy
Yes
No
No
Individual

Michael Falvo
Independent Electricity System Operator
Yes
No
No
Individual
Greg Froehling
Rayburn Country Electric Cooperative
Yes
No
Yes
Comments: Although it may not seem apparent since the focus has been on Medium and High implementation. It is important to note there is no implementation period identified for newly identified Low BES Cyber Assets. With uncertainty around Low BES Cyber Asset determination I feel it would be prudent to identify this situation and assign a period to develop cyber security policies where none may have existed before. The situation could arise during an audit when it is asserted by the entity that they have no Low BES Cyber Assets and the auditor disagrees… at that point it could be a potential violation unless there is a period of implementation to develop cyber security policies. Keeping in mind that FERC allowed an additional year for the Low BES Cyber Assets to develop and implement cyber security policies, I suggest using the timeframe for newly identified medium and high and adding time as the original FERC approved effective date for CIP V5 did.
Individual
Roger Paschall
Texas Reliability Entity
No
I think the Standards Drafting Team should have the flexibility to reduce ambiguity and enhance clarity in any of the existing CIP v5 requirements. There is a significant amount of ambiguous language in CIP v5 and any lessening of that ambiguity can only increase reliability of the BES.
No

Yes
The SAR is focused on the actions of ten people from utilities and three NERC staff members whose SDT performance is a part-time function from their existing suite of responsibilities but whose actions can impact the entirety of the Bulk Electric System and most of the North American general public. That's a lot of responsibility to give to part-timers and expect a world-class product in less than twelve months. I think the SDT should be increased for this specific project by at least an additional eight people, one from each Regional Entity. Personnel from the Regional Entities are independent and cannot be perceived as working for the benefit of the utilities themselves.
Individual
Thomas Foltz
American Electric Power
Yes
No
Yes
Identify, assess, and correct wording modifications: AEP does not have concerns with the removal of the “identify, assess, and correct” language. This wording can be removed and effectively handled by the Reliability Assurance Initiative and the Find, Fix and Track process as necessary. Security controls for Low impact assets: AEP does not believe it is in the best interest of the industry to prescribe security controls for Low impact assets at this time. FERC presented NERC with 4 options for addressing security controls for Low impact assets. AEP recommends NERC request FERC to allow the ERO to conduct a study during the NERC transition study or CIP Version 5 transition program to assess the cyber security programs documented and implemented by entities with Low impact assets. This would provide NERC the visibility needed to determine if specific cyber security controls, a more refined list of criteria for cyber security programs, or industry guidance would help to improve the cyber security posture of Low impact assets. Many entities will be implementing cyber security programs for the first time under CIP version 5 over thousands of assets. These assets will vary in complexity from computer or server in a controlled room environment to protective relays or single loop controllers located in large open areas. The industry will need time to refine their security programs around the varying locations. If more prescriptive controls are written for Low impact BES Cyber Systems the implementation plan should be revised accordingly to allow industry appropriate time to achieve the controls. Communications network: AEP is concerned that the scope and cost of compliance with the NERC CIP standards could increase significantly with little improvement in reliability to the BES if the definition of communications networks and security controls associated with those networks is not addressed properly. NERC should consider the guidance provide by industry in the NERC led technical conferences on 1/21/2014 and 1/23/2014: 1. Consider the risk the

communications network poses to the BES a. This should not be a one-size fits all. Communications networks that present a greater risk should require increased security. 2. Exclude external networks not owned or operated by the entity (e.g. Telecommunications company owned leased lines) 3. Excluding signaling communications (e.g. 4-20 mA, differential voltage, and contact closures) 4. Consider where the communications network resides: a. Does it reside in a control center? b. Does it reside in a generation facility? c. Does it reside in a transmission facility? d. Does it traverse public areas? 5. Review the standards and physical security controls FERC mentioned: a. NIST sp800-53 rev3 control PE-4 b. ISO-27001 control A.9.2.3 c. locked wiring cabinets, disconnected or locked spare jacks, or protection of cabling by conduit or cable trays 6. Avoid complex technical issues like encryption. This technology is difficult to implement in control system environments and may have adverse reliability impacts if implemented incorrectly. Transient Devices: AEP is concerned with the Commission's decision to require security controls for transient devices. The target of the NERC CIP standards should be the BES Cyber Systems. The NERC CIP requirements protect the BES Cyber Systems through a defense in depth strategy that includes cyber security programs, awareness and training programs, physical security, remote access control, local access control, security patch management, malware prevention, cyber security incident response programs, and etc… A standard that requires a similar set of security controls for transient devices would be difficult for an entity to prove compliance with in an audit. By definition transient devices are not connected for an extended period of time to cyber systems where they can be monitored and logged this would prevent the proper documentation of compliance evidence for an audit. AEP requests NERC to revisit the transient devices with FERC to address the auditability concerns and highlight the fact that existing security controls that are required by CIP-003 through CIP-011 will adequately address the security concerns posed by transient devices.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
Yes
No
Yes
ATC recommends the following for consideration by the Standards Drafting Team:• Modify the text in the last paragraph of the SAR 'Detailed Description' section to consider input from the industry regarding obvious modifications or finite errors that should be made to the CIP standards while they are 'open' for revision. ATC recommends to modify the last paragraph to read: "When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 transition activities, such as from the NERC transition study or CIP Version

5 transition program, including input from the industry regarding obvious modifications (e.g. typographical errors, vital clarifications, or clear contradictions).”
Group
NERC Standards Review Forum
Russ Mountjoy
Yes
No
Yes
The MRO NSRF recommends that NERC allow flexibility in the schedule and place priority on responding to the directives related to the “identify, assess, and correct” language and communication networks by February 3, 2015. While an approach and subsequent filing that addresses all four FERC directives is preferred, it might not be feasible given the complexity of the issues. Consider modifying the text in the last paragraph of the ‘Detailed Description’ section to also give the SDT the option of considering input from the industry regarding obvious modifications that should be made to the CIP standards while they are ‘open’ for revision. Obvious modifications could include typographical errors, crucial clarifications, and the correction of clear contradictions. Since the input is informal, the SDT would not be obligated to consider the input or provide any justification for its rejection. We suggest revised wording to read, “When developing these new or modified CIP standards, the SDT may consider input from CIP version 5 Transition activities, such as from the NERC transition study or CIP Version 5 transition program. Include informal input from industry regarding obvious modifications (e.g. typographical errors, vital clarifications, and clear contradictions).”
Group
WECC
Steve Rueckert
Yes
No
No
Individual
Judy VanDeWoestyne
MidAmerican Energy Company

Yes
No
No
Individual
James Gower
Entergy
No
Comments: 1.)Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements. Response: Entergy supports entities ability to have the flexibility to correct self-identified issues that have minimal to no impact on the Bulk Electric System, such as documentation issues, and believes this language should remain in the standards. 2.)Develop modifications to the CIP standards to address security controls for Low Impact assets. Response: Applying security controls at Low Impact assets would have virtually no practical risk reduction value and would be done purely for the perceived benefit. 3.)Develop requirements that protect transient electronic devices. Response: Entergy’s position is that transient devices are not assets that comprise the Bulk Electric System, and therefore are outside the scope of the NERC CIP standards. Any risk these devices pose is already mitigated by compliance with the existing CIP standards for cyber assets that are within NERC CIP scope. 4.)Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks. Response: No comments
No
No
Individual
Nazra Gladu
Manitoba Hydro
Yes
No
Yes

(1) Manitoba Hydro is of the view that including IAC language in the text of NERC reliability standards may create confusion regarding the duty to comply and introduce conflicts with North American legislation imposing an obligation to comply with NERC standards. Thus, Manitoba Hydro supports the removal of the IAC language. Therefore, Manitoba Hydro believes that the option to modify the IAC language should be eliminated from the SAR. In the January 8th, 2014 letter from F. Gorbet on behalf of the NERC BOT to John Anderson of the MRC requesting policy input to the BOT, Gorbet states that “NERC supports drafting team removal of the IAC language…”. The SAR should be revised accordingly. (2) The word “Low Impact” is not defined in the NERC Glossary of Terms, and as such should be defined, or de-capitalized. (3) Detailed Description, first bullet - add quotation marks around the phrase “identify, assess, and correct” for consistency with the rest of the SAR.
Individual
Bill Temple
Northeast Utilities
Yes
No
Yes
1. Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements. Northeast Utilities recommends removing this language from the standards. These activities are more appropriate for enforcement activities or events analysis. 2. Develop modifications to the CIP standards to address security controls for Low Impact assets. Northeast Utilities recommends the SDT develop a new standard that will allow this one standard to have an implementation date later than the other V5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. 3. Develop requirements that protect transient electronic devices. Northeast Utilities recommends drafting a definition based on impact to BES for transient devices and categories for device types. NU recommends that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other V5 standards. 4. Create a definition of “communication networks” and develop new or modified standards that address the protection of communication networks. Northeast Utilities recommends that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards.
Individual
Tracy Richardson
Springfield Utility Board

Yes
No
No
Individual
Clifford Johnson
Consumers Energy
No
Items 2 and 3 of this SAR do not have a timeframe for completion and provide no additional direction or goal for the outcome. For item 2, entities do not require a detailed list of controls to develop the required policies. Entities are more than capable of utilizing cyber security best practices and the requirements laid out in CIP-003 through CIP-011 as guidelines or starting points for developing the policies required for the lower, and in some cases virtually zero impact assets. CIP-003-5 R2 lists specific subjects that must be covered. These are cyber security awareness, physical security controls, electronic access controls (external routable and dialup) and incident response. These basic requirements are adequate direction for entities to proceed. There is no need for greater, more prescriptive details. Additionally, the “policy” development requirement is highly appropriate due to the somewhat “catch-all” aspect of the Low Impact category. These security controls will apply to hundreds, if not thousands, of Low Impact devices often in remote, unmanned locations and the importance and reliability impact of these will vary greatly. The volume of Low Impact assets make further prescriptive requirements unmanageable and causes substantial regulatory burden. Many of the Low Impact assets will have no external connectivity whatsoever. At most if not all entities, these assets are either located in locked cabinets or located in locked buildings inside fenced and locked substations. In addition to the low impact, (if not nearly-zero in many cases), the overall risk (threat, vulnerability, cost/impact) of/to these assets is in general, negligible. Again, modification to the CIP standards to address security controls for Low Impact assets could add complexity, if requirements beyond policy development are mandated. Item 4 has the potential to create significant undue burden on entities. In general, much of the communication systems utilized today are over public carrier where entities have extremely little control beyond negotiated service level agreements and virtually no way of validating if the carriers are securing these systems from day-to-day. It would seem more appropriate, that requirements for these systems be included in other, yet-undeveloped CIP standards, or a new set of standards specifically addressing these types of systems. In either case, these other standards should be specifically applicable to these telecommunications carriers as well.
No

No
Individual
RoLynda Shumpert
South Carolina Electric and Gas
Yes
No
Yes
1) NERC needs to clearly address, with justification, specific implementation timeframes/deadlines within this SAR. The initial CIP V5 standards were approved by the industry with effective dates that were directly associated with the scope of work prescribed by CIP V5, as written at the time of proposal. This SAR will introduce new standards and/or enhance the current CIP V5 standards, thereby increasing the prescribed work scope (and potentially require re-work). Additionally, resources that are focused on CIP V5 implementation will now have additional workload in order to participate in the Standards Development Process associated with this SAR. This was not anticipated when the initial CIP V5 effective dates were approved by the industry; therefore, the CIP V5 effective dates must be revisited given the extent of change with 17 requirements being modified (IAC removal) and new requirements (and potentially new standards) being promulgated. These new requirements (and standards) will affect the current requirements being implemented. 2) NERC needs to provide guidance to the industry on how to handle Low Impact BES Cyber Systems (and communications networks) while this SAR is being developed. Due to the aggressive implementation dates specified in CIP V5, the industry cannot wait to work on applying security controls to their Low Impact Assets. This SAR will develop a set of security controls that must be applied to Low Impact BES Cyber Systems. The current CIP V5 standards allow each entity to define their own security controls to address broad subjects. NERC needs to promote consistency in implementation by providing the industry an extension on Low Impact Assets and communications networks that coincides with the development this SAR, so that a defined set of security controls can be developed and then implemented by the industry. 3) NERC needs to include in this SAR a provision whereby NERC must provide timely guidance to the industry on how the CIP V3 to CIP V5 transition is to take place. NERC must also provide implementation time leeway, per the Transition Study, for entities to migrate from V3 to the modified V5.
Group
Duke Energy
Michael Lowman

Yes
No
Yes
(1) Duke Energy would like for the drafting team to consider creating separate standard(s) and requirements that address security controls for Low Impact Assets. We believe this would better simplify the monitoring and enforcement process. (2) We ask the SDT to clarify the meaning and intent of protecting transient electronic devices. Is the intent to protect the transient devices themselves or the devices that connect to those identified transient devices? (3) When developing a definition of communications network and determining what to protect, the SDT should ensure that “integrity, confidentiality, and availability” are maintained as principles in the development. (4) In the development of the scope and definition of communication networks, we would like the SDT to consider the following items: a. Identify the ownership line of demarcation for compliance when multiple Owners are involve such as i. Vendors ii. Other Registered Entities iii. Wireless iv. ESPs v. Point-to-point networks vi. Logical vs. Physical networks vii. encryption/VPN communications viii. trusted vs. non-trusted networks b. further break down of the definition to include: i. entity-owned ii. intra-entity iii. vendor-owned iv. Analog v. serial-to-fiber vi. TCP/IP fully enmeshed
Individual
Ayesha Sabouba
Hydro One
No
The SDT should provide a definition for "transient electronic devices".
Yes
The Ontario Energy Board is also looking at cyber security requirements for utilities within Ontario, Canada. I am not sure how far they have progressed, however.
No
Individual
Steve Karolek
We Energies d/b/a Wisconsin Electric Power Company
No
While we understand NERC’s desire to make progress on all of FERC’s Order 791 directives, it is important to ensure that resources are focused first and foremost on those which are time-bound and that those directives not due in one year should not be worked on to the detriment of doing a good job addressing those which are due in one year. FERC recognized the sensitivity and complexity of these areas when they chose to not put a time box on

them. As an industry we need to make sure we spend the appropriate time considering and addressing these issues.
No
Yes
* As the drafting team “considers whether any further standard protections are needed to address potential vulnerabilities associated with transient devices (e.g., thumb drives and laptop computers)” they should remember that thumb drives are not themselves Cyber Assets/Systems and the need may be less to protect thumb drives than to protect Cyber Assets/Systems from thumb drives. Additional protection for information on thumb drives may also be in order but that falls in the realm of information protection not transient device protection. Thumb drives should not be considered to be transient devices. * The applicability section (4) should be updated to remove section 4.2.2 for the reasons previously documented by We Energies’ Howard Rulf and also should be updated to specifically exempt small distributed generation with aggregated capacity less than 75MW (e.g. individual wind turbines). [Howard Rulf’s previously documented comments: Section 4.2.2 wording means that for all entities other than DP, the standard applies only to their BES Facilities. A BES Facility is essentially equipment operating at >100 kV that is connected to the BES by terminals. Nothing in a Control Center is >100 kV connected to the BES by terminals. These standards will only apply to entity functions that own equipment operated at >100 kV and are connected by terminals (i.e. generators, transmission lines, high voltage transformers, etc.).]
Individual
Richard Vine
California ISO
Agree
IRC's Standards Review Committee
Individual
Chris Scanlon
Exelon
No
Under Industry Need, item #1: “Modify or remove the “identify, assess, and correct” language in 17 CIP version 5 requirements.” Removal of the “identify, assess, and correct” (IAC) wording without any replacement wording to promote compliance enforcement maturity that allows very strong programs with very minor variances to be compliant is problematic. The IAC language was essential for entities to support approval of the CIP Version 5 Standards. While FERC Order 791 requests that compliance language be removed from the requirements, the IAC language in the requirements may need to be replaced with language elsewhere in the Standards, such as in the Measures, to reflect the underlying purpose of the IAC language. Proposed Revision: “Modify or replace the “identify, assess,

and correct" language in 17 CIP version 5 requirements."Under Industry Need, item #3: "Develop requirements that protect transient electronic devices." The scope needs clarification. Protecting transient devices should not be the focus of this activity, but rather protecting the Bulk Electric System reliability from risks that may be introduced by use of a transient device. While protecting the Bulk Electric System would likely include some controls on the transient devices to avoid risk to BES Cyber Systems and the Bulk Electric System, focus of the controls and other potential requirements will be better designed with the proper scope wording that does not focus protection on the transient assets. Proposed Revision: "Develop requirement(s) that protect the Bulk Electric System reliability where transient electronic devices (not classified as BES Cyber Assets as described in BES Cyber System definition) are used." Note For Reference the BES Cyber System Definition - A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes.) Detailed Description, bullet #3: "The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP Standards." This action may create a timing problem for the SDT. Ideally, the SDT will work on all four Directive areas concurrently, to the degree possible, and the SDT may be able to address the issues identified within Order 791 before the survey results are available. Proposed Revision to the last sentence of the bullet: "The SDT shall review information from this survey, as available during the Standards development process, for relevant and timely insight to the development of new or modified standards associated with transient devices."Detailed Description, bullet #4: "The SDT shall review the technical conference testimony and comments to inform the development of the definition for communication networks and a new or modified standards for the protection of communication networks." Again, this may create a timing issue for the SDT. Order 791 directs a one year timeframe for communication networks, thus requiring the SDT to move quickly on the development work. Recognizing that this is a FERC led conference and not controlled by NERC, the action item should allow for flexibility. Proposed Revision to the last sentence of the bullet: "The SDT shall review the technical conference testimony and comments as available during the Standard development process for relevant and timely insight to the development of new or modified standards for the protection of communication networks."Definitions are part of the Standard: It may be useful to include a note in this SAR stating that a modification to a CIP definition(s) is considered a modification to a Standard. This would clarify that if an issue can be addressed with only a change to a definition that would be acceptable under this SAR. VRF/VSL: If the SDT will be working on revisions to the VRF &/or VSLs that should be stated in the SAR. Language Tweaks: Industry

Need: to clarify that the SAR language summarized the Order 791 directive details, consider adding that note as follows: On November 22, 2013, FERC issued Order No. 791, Version 5 Critical Infrastructure Protection Reliability Standards. In this order, FERC approved version 5 of the CIP standards, and also directed that NERC make the following modifications to those standards (as summarized from FERC Order 791): Industry Need Typo: Last sentence in the Industry Need section, “time frame” should be one word as it is later in the Detailed Description. Brief Description: While it may be unlikely, the SAR should not preclude use of another standard or standard revision to address a FERC directive. For instance, a standard for protection of communication networks could fall within the COM standards family. Consider including the added phrase to read as follows: “The proposed project will develop new or modify existing requirements in the CIP standards, or other NERC Reliability Standards if determined the best approach, to address the directives from FERC Order No.791. This project may also consider input that may be provided from CIP version 5 transition activities, for example from the NERC transition study or CIP Version 5 transition program.”Detailed Description: The description should further emphasize that the scope of SDT work is to address those concerns raised in Order 791. Please consider including the added phrase to read as follows: “As stated above, the purpose of the proposed project is to respond to the directives in the FERC Order 791 and to respond within a timeframe required by the order for the directives related to “identify, assess and correct” language and communication networks. The following is a description of the responses the standard drafting team (SDT) shall consider during development of new or modified standards to address the concerns raised in Order 791: …”Detailed Description: In the fourth bullet, the first sentence is missing a word and “communications” should be singular: “The SDT shall consider how to define the term “communication networks” and develop new or modified …”
No
No
Individual
Michael Haff
Seminole Electric Cooperative, Inc.
No
Seminole agrees with comments provided by the National Rural Electric Cooperative Association (NRECA).
No
Yes
Seminole agrees with comments provided by the National Rural Electric Cooperative Association (NRECA). In addition, Seminole believes that two separate issues (transient

devices and definition of BES Cyber Asset) have been inappropriately combined and should be addressed separately. Seminole supports the survey to identify the 15-minute parameter issues for FERC. Seminole believes that separation of these two issues would allow the following: 1. An independent review of the 15 minute parameter; and 2. A determination of what should qualify as a transient device, and what controls should be put into place for those devices It will be difficult to combine the 15 minute standard and transient devices directly. Any device plugged into the ESP will need to be a Cyber Asset because misoperation or malware would have the ability to impact the Facility within 15 minutes. The 30-day window goes away other than the parenthetical footnote in the definition. That was FERC's objection. Combining two separate issues in this way confuses the matter that the team was directed to address in Order 791.
Individual
Amelia Sawyer
CenterPoint Energy
No
The following statements on page 3 of the SAR exceed what is directed in Order 791:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."Paragraph 124 of Order 791 directs "NERC to conduct a survey of Cyber Assets that are included or excluded under the new BES Cyber Asset definition during the CIP version 5 Standards implementation periods. Such data will help provide a better understanding of the BES Cyber Asset definition. Based on the survey data, NERC should explain in an informational filing the following: (1) specific ways in which entities determine which Cyber Assets meet the 15 minute parameter; (2) types or functions of Cyber Assets that are excluded from being designated as BES Cyber Assets and the rationale as to why; (3) common problem areas with entities improperly designating BES Cyber Assets; and (4) feedback from each region participating in the implementation study on lessons learned with the application of the BES Cyber Asset definition." CenterPoint Energy recommends deleting the statements, ""During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards." as the statements and survey are not related to the currently directed modifications or activities of the SDT. Based on Order 791, the directed survey and its results are for an informational filing and future consideration by the Commission. Using the survey results to inform the development of the new or modified standards may add an unnecessary level of complexity, frustrate the process, and delay the final deliverable.
No

No
Group
Electric Reliability Compliance
Josh Andersen
Yes
No
Yes
CIP-008 - Requirement R1. Part 1.1 : Salt River Project recommends that NERC develop the standard classification for identifying Cyber Security Incidents. Because this is left up to each entity, it leaves room for discrepancy. Therefore there could be an inconsistency in classification and reporting amongst the industry entities. Additionally, by creating a standard and consistency, entities would be able to better collaborate in prevention, detection and eradication methods to protect the bulk electric systems. CIP-011 – General Note : While the development of requirements for Low Impact Cyber Systems might be on the roadmap as part of the larger effort to address security controls for these systems, Salt River Project recommends that NERC either provide specific information protection requirements for Low Impact BES Cyber Systems or exclude them from the requirements.
Individual
Michelle R. D'Antuono
Occidental Energy Ventures Corp.
No
Occidental Energy Ventures Corp. (“OEVC”)agrees that the SAR captures FERC’s primary intent in Order 791. In addition, we are aware of the limited time frame that has been given to NERC and the industry to address several of the rulings. Unfortunately, the Commission’s directive to eliminate the risk-based qualifier in 17 requirements eliminates one of the major reasons why we voted to approve CIP Version 5 to begin with. However, our reading of Order 791 indicates that FERC is willing to accept other equally effective alternatives to the “identify, assess, and correct” language. As such, we found it disheartening that the SAR drafting team seems to propose a solution which mostly involves the education of stakeholders by ERO Compliance and Enforcement staff. In OEVC’s view, this is not sufficiently binding to those organizations – who will be free to change their oversight approach as they see fit. We are not suggesting that NERC or the Regions will make alterations lightly, but our experience of the CAN process and other similar initiatives has been that they are not rigorous enough. We ARE suggesting that the SAR must be updated to capture the goal that a definitive and binding review/acceptance compliance process

must be developed. In fact, the NERC Rules of Procedure may be a candidate. It was updated to allow for individual exceptions to allow appeals related to the Definition of the BES – a project that was at least as complex and controversial as this one is.
No
Yes
The focus of the CIP v5 revisions initiative must be placed on the two items that FERC has assigned a due date (remove the “identify, assess, and correct” language and address communication networks). In OEVC’s view, both of these are substantial modifications that deserve the development team’s full attention. This means that the remaining two items (create security controls for Low Impact assets and requirements that protect transient electronic devices) should be deferred to Phase II of the project. We recommend that the SAR be updated to reflect this realistic development approach.
Individual
Barry Lawson
National Rural Electric Cooperative Association (NRECA)
No
NRECA’s comments focus on ensuring the SAR accurately represents the FERC directives in Order No. 791. In the “Industry Need” and “Detailed Description” sections the following revisions should be made: (1) the language used in the SAR for Low Impact assets should be revised to remove references to security controls specificially, and replaced with “……address the lack of objective criteria against which NERC and the Commission can evaluate the sufficiency of an entity’s protections for Low Impact assets”; (2) the language used in the SAR for transient devices should be revised to say “…….develop either new or modified standards to address the reliability risks posed by connecting transient devices that fall outside the BES Cyber Asset definition to BES Cyber Assets and Systems”; (3) the language used in the SAR for communications networks should be modified to state that the focus is on nonprogrammable components of communication networks; and (4) the language in the first line of the last bullet under “Detailed Description” should be revised to state “Create a definition of “communication network”……..”
No
Yes
What role will the SDT have in developing the survey for transient devices? The SDT should collaborate with NERC to develop the survey and this should be stated in the SAR. The SAR should make reference to the forthcoming order on clarification and rehearing and state that the SDT will factor this in to their work.
Group
ACES Standards Collaborators

Trey Cross

Yes

(1) We support NERC's efforts in modifying the NERC CIP Version 5 Standards to address FERC directives regarding "identify, assess, and correct (IAC)" language, Low Impact requirements, protection of transient devices, and communication network definitions. Removal of the IAC language will eliminate uncertainty of auditing the requirements that contain this language. Any standard or requirement should have clear, concise, and auditable language that is consistently applied across all NERC regions. (2) However, the implementation plan is unclear. Are registered entities going to have to comply with the current IAC language before it is modified since the standards are approved? We ask that the SAR drafting team consider these implementation issues and provide guidance during the development of this standard.

No

Yes

(1) We are concerned that modifying the 'IAC' language will delay version 5 implementation efforts for internal controls and would like NERC to provide guidance how to build internal controls based upon the Reliability Assurance Initiative (RAI) as soon as possible. Specifically, guidance needs to be provided for those requirements that relate to low impact BES Cyber Systems and high frequency violated requirements that IAC was written to address. Without the IAC language, the CIP version 5 standards could result in zero defect compliance for each deviation from a requirement. We support NERC's focus on internal controls and would like to see formal guidance issued during the interim period while this drafting team is revising the version 5 standards. We appreciate that NERC has stated publicly that they are committed to a non-zero defect policy and are hopeful the implementation studies and transition guidance will provide ultimate clarity around this issue. (2) As addressed in question 1, we support NERC's focus on standards that are clear, concise and auditable. The Version 5 Standard Drafting Team wrote the current Low Impact requirements in a non-prescriptive manner to allow for entities that do not currently have Critical Assets as defined in CIP Version 3 to build a customized compliance program based on the limited risk they pose to the Bulk Electric System. We support NERC's effort to allow small entities the flexibility to interpret those requirements that match their infrastructure, resources and program size; however, that flexibility must also be consistently audited across all regions. NERC should develop requirements that provide small entities and auditors a baseline of compliance to remove the possibility of differing interpretations of compliance for the Low Impact requirements. (3) Regarding the FERC directive that addresses requirements for transient devices, we understand that this is a complicated issue with many questions that need to be answered, e.g., "what is the definition of a transient device, what are the time requirements that qualifies a device to become a transient device, is a laptop considered a transient device, etc. Given the spectrum of devices, timing and other considerations for cyber assets to be a possible transient device, we recommend that any definition of a

transient device includes supporting documentation that provides examples of what is and what is not considered a transient device to remove any uncertainty. (4) ACES recommends that NERC use an industry definition of network communication in order for entities to leverage existing standards, definitions, and network configurations. NIST 800-82 has been industry vetted and written specifically for industrial control systems (ICS). Their definition of a control network is: “Those networks of an enterprise typically connected to equipment that controls physical processes and that is time or safety critical. The control network can be subdivided into zones, and there can be multiple separate control networks within one enterprise and site.” Furthermore, standard requirements written for communications networks need to have clear boundaries about what is included and what is not included. What is included must be under the registered entity’s control. For example, this cannot become a standard that requires a registered entity to ensure the communications infrastructure of their telecom provider is CIP compliant. In other words, the standard cannot become a national or international telecommunications infrastructure standard. (5) We support the use of this definition in that is specifically speaks to ICS functionality, assets and cyber asset that run a facility.
Group
Bonneville Power Administration
Andrea Jessup
Yes
No
No
Group
Arizona Public Service Company
Janet Smith, Regulatory Affairs Supervisor
Yes
No
AZPS does not have familiarity with any Canadian provincial regulatory
No
The thoughtful implementation of new or revised standards is just as critical as the content of the standards themselves. Therefore, AZPS urges the Standards Drafting Team to ensure that any new or modified standards are also accompanied by a transition and/or implementation timeline that best matches the magnitude of the proposed changes. Bearing in mind those entities with a large number of BES assets may need more time to implement

any associated changes than entities with relatively few BES assets. AZPS is appreciative of NERC's efforts on the CIP Version 5 Implementation Pilot program and thus requests that the lessons learned from those pilots be considered by the drafting team as it develops modifications to the CIP standards. Incorporating lessons learned now will yield valuable perspective and may prevent rework later. In addition, AZPS further urges the SDT to be mindful of not only the technical aspects of the modifications to the standards but also the auditability of control effectiveness as applied to the intent of the standard. Doing so would help to ensure the technical processes are sufficiently clear and can also be easily documented – both of which are of critical importance. Lastly, AZPS is supportive of NERC's efforts with respect to the Reliability Assurance Initiative and its movement away from the "zero tolerance" approach. AZPS requests that NERC and the standards drafting team make modifications or develop an approach the can be consistently applied across all NERC standards.
Individual
Kenn Backholm
Public Utility District No.1 of Snohomish County
No
Recommend modifications to the SAR language to clarify and align with FERC order 791: SAR, page 3:"During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the "15-minute" parameter. The SDT shall review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards."• Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices.• Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR. Recommends the following be considered: i) Suggest changing the Detailed Description's second bullet to The SDT shall consider the development of necessary Standard modification or new Standards that address security controls for Low Impact assets. ii) Suggest splitting the Detailed Description's third bullet into two bullets for clarity. Replace this third bullet with the following a - c. a) The SDT shall consider how to define the term transient device. b) The SDT shall consider whether further Standard protections are needed to address vulnerabilities associated with transient devices. c) The SDT will review the results of the ERO survey concerning the use of the "15 minute" parameter to inform the SDT's development of a new / modified Standards for the protection of Cyber Assets and BES Cyber Systems from the vulnerability introduced by transient devices.
No

Yes
NERC staff requested that the industry not submit Requests for Interpretation (RFI). However, more detailed reviews of the approved CIP Version 5 Standards generated additional questions regarding compliance. NPCC members are requesting a process for seeking clarifications so that company implementation expectations of CIP Version 5 will be consistent with future audit expectations. Recommend removing the “identify, assess, and correct” language in 17 CIP Version 5 requirements. Recommend that the Standard Drafting Team develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Low Impact assets, like substations, are often shared by multiple entities making personnel requirements of CIP-004-5 extremely onerous. Physical security costs will probably be the biggest component of spending for compliance. It would be best if only certain areas of the facility (i.e. those with cyber assets) be protected, not the whole asset. Recommend drafting a definition based on impact to BES for transient devices and categories for device types. Recommend that the SDT develop a new standard that will allow this one standard to have an implementation date later than the other Version 5 standards. Recommend that the SDT develop a new standard to address communication networks that will allow this one standard to have an implementation date later than the other V5 standards. Recommend clarifying the applicability of CIP-002-5. Registered Transmission Operator (“TOP”) are automatically classified as a medium impact through application of Attachment 1, however some registered TOPs do not have any BES Cyber Assets under the Definition: “A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.”Through registration and application of section 2.12 of Attachment 1, a TOP is automatically selected to the medium impact rating; however some registered TOPs may not have any BES assets that can impact the reliable operation of the BES. Based on discussion with subject matter experts at NERC and WECC there appears to be confusion on how to address this issue. In addition to clarifying CIP-002-5, it would be helpful for NERC or the Regional Entities to review or validate Registered Entitles CIP-002-5 assessment prior to the version 5 implementation so the RE has time to address CIP v5 requirements. Although there is an implementation plan, it is clear that going from no Critical Assets in CIP v3 & v4 to a medium impact will require significant funds, resources, and schedule.
Individual
paul haase
seattle city light
No
Regarding following language: “During the development timeframe, the ERO will conduct a survey to determine the number of assets, by type, that fall outside the definition of BES Cyber Asset because the assets do not satisfy the “15-minute” parameter. The SDT shall

review the results of this survey to inform its development of new or modified standards for the protection of transient devices or other elements of the CIP standards." Paragraph 124 of Order 791 directs a survey to identify systems that would be excluded by the 15-minute criteria. The directive for the survey does not address transient devices. Paragraph 136 of Order 791 directs the creation requirements to address the risks of transient devices that are attached to BES Cyber Asset for less than 30 days. The 15-minute criteria and the 30-day criteria address differing types of assets and should not be merged together as noted on page 3 of the SAR.
No
No

Additional Comments:

Idaho Power
Molly Devine

1. No
Comments:

The scope of the SAR should be expanded to include a revision to the CIP-002-5.1 standard that will clarify the process that should be followed to identify BES Cyber Systems. The CIP-002-5.1, standard as currently written, creates a great deal of confusion and uncertainty around how to proceed or how to maintain compliance with the standard.

2. Yes
Comments:

In order to successfully implement any new requirements surrounding communications networks that connect Canadian and US utilities one of two options must be used. 1. The connections between the utilities must be exempted from requirements or 2. the Canadian provinces must implement the same requirements. For example if a new requirement that is approved that involves encrypting communication data over a communications link that is physically crossing the international border between a Canadian utility and a US utility but is only required by the US utility. Only requiring the US utility to implement encryption on the communications link while not requiring the Canadian utility to do the same will create many difficulties, challenges and confusion. Additionally, the cost and implementation details may be contentious to the Canadian utility and leave both utilities in a bind of how to implement and support systems that are deemed "critical".

3. Yes
Comments:

The development of standards surrounding communication networks needs to be done carefully and clearly as these topics start to touch upon issues that have previously been excluded from the CIP standards and will need to be fully vetted. NERC should consider defining different regulations for utility owned communications versus leased facilities from external entities. Each of these two scenarios pose separate challenges and risks and need thoughtful consideration taking into account the fundamental differences of what is in the utility's control and what can and will need to be addressed with external providers. Additionally, there is no single reliability standard that addresses "communications networks". Instead, the various communications network requirements are sprinkled throughout the NERC reliability standards (e.g. COM, PRC, TOP, CIP, etc.). There should be an effort made to have a consolidated standard (or set of standards) for "communications networks" owned by Functional Entities. There is also a great deal of concern over the appearance that NERC's seems to be viewing the only option as removing the "identify, assess, and correct" language rather than considering other options. Although, there has been more communication as of late about the RAI there needs to be a more concerted effort to move away from the zero-defect approach in some fashion to allow the entities to protect and not just comply.