Name (60 Responses)
Organization (60 Responses)
Group Name (36 Responses)
Lead Contact (36 Responses)
Question 1 (86 Responses)
Question 2 (86 Responses)
Question 3 (85 Responses)
Question 4 (0 Responses)
Question 4 Comments (96 Responses)
Question 5 (87 Responses)
Question 6 (86 Responses)
Question 7 (86 Responses)
Question 7 Comments (96 Responses)
Question 8 (0 Responses)
Question 8 Comments (96 Responses)
Question 9 (85 Responses)
Question 10 (87 Responses)
Question 11 (86 Responses)
Question 12 (0 Responses)
Question 12 Comments (96 Responses)
Question 13 (87 Responses)
Question 14 (86 Responses)
Question 15 (0 Responses)
Question 15 Comments (96 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
No comment
Yes
Yes
Yes
no comment
no comment
Yes
Yes
Yes
no comment
Yes
Yes
no comment
Group
Northeast Power Coordinating Council
Guy Zito
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not

accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”. For R1.3, and R1.4 wording needs to be added to state that physical security incidents need to be included as well as for Cyber Security Incidents.
No
No
No
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated Implementation Plan’s Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure Recommend changing from the reference from “R1.2” to “Part 1.2” in R3 Part 3.4 for correctness.
No
No
No
Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc.” instead of “device drivers, DLL, applications included in an operating system or package, etc.?” Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? Request clarification on R1 Part 1.3. Each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part). Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways. In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity. For R2 Part 2.1, recommend the previous Version 5 words since this updated Part is not understandable. Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment. Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low”. Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That

VRF is “medium” while the Requirements and Measures shows R2 as “low”.
Yes
No
The second paragraphs of R2 Parts 2.1 and 2.2 are the same. Recommend removing them from Parts 2.1 and 2.2, and make a into a new Part 2.3 for clarity.
Individual
Frank Dessuit
NIPSCO
No
Yes
Yes
NERC should clarify why the word “dated” has been added to the measures used throughout this requirement. NERC should clarify the use of “reliability tasks” in this proposed standard, specifically, whether they are the same “reliability tasks” as required by PER-005. NERC should provide clarification on the terms “Cyber Security Incident” and “Reportable Cyber Security Incident”.
No
Yes
Yes
NERC should provide a definition of the term “recovery,” and whether it is meant to apply to disaster recovery / business continuity focusing on recovery of functionality or capability of a system, or to restoration after an individual asset loss, or both.
Yes
Yes
Yes
R1 indicates a process for a change occurring. NERC should clarify if R2 identifies an undocumented change, would a self report be required, or is the “document and investigate” language of R2 intended to eliminate the need for self reports to R1? NERC should also clarify whether all VAs must be performed prior to the CIP V 5 effective date, and whether entities have an additional year or 3 years from the effective date.
Yes
Yes
Individual
Thomas C. Duffy
Central Hudson Gas & Electric Corporation
Yes
Yes
Yes
No
Yes
Yes
Requirements 1.1, 1.2, 1.3 and 1.5: The applicable 'systems and assets' for these requirements should be changed from 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems at Control Centers' to agree with the rest of the requirements of the standard. All the requirements should apply and they should apply only to Control Center assets.
No
No

No
This standard should not be applicable to all 'Medium Impact BES Cyber Systems'. It should be applicable to only 'Medium Impact BES Cyber Systems at Control Centers' and 'Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity'.
Yes
Yes
Individual
Michael Falvo
Independent Electricity System Operator
Yes
Yes
Yes
No
No
Yes
CIP-009-5 R1, Part 1.3: – IESO suggests the change of word “recover” to “restore” outlined within the requirement. CIP-009-5 R1, Part 1.4: IESO suggests the change of word “recovery” to “restoration” outlined within the requirement. We also suggest that the following terms should be defined: recover recovery, restore and restoration. CIP-009-5 R2 - Part 2.2: IESO believes the usage of “backup media” is antiquated and most entities use redundancy for restoration. The use of redundancy for restoration should be referenced, or the backup media should be defined to include the new technologies.
No
No
No
CIP-010-1 R1 - Part 1.4.1: An entity could face double jeopardy in that non compliance with this requirement means non-compliance with the requirements in the referenced standards. CIP-010-1 R1 - Part 1.5.1: The “where technically feasible” clause is not applicable here; therefore, IESO is recommending the removal of this clause from this requirement. CIP-010-1 R2 - Part 2.1: Unless the term “continuously” is defined, IESO recommends the removal of this word from the requirement.
Yes
No
CIP-011-1 R2 - Part 2.1: IESO recommends that the requirements outlined here should be broken out into two separate sections: one for cyber assets that contains BES Cyber System Information (i.e. network diagram) and the other pertaining to Cyber Assets within an ESP.
Group
Comment Development SME list
Gerald S. Freese
Yes
Yes
Yes
Yes
Yes
Yes
1. R1.3- In the requirement, the word “recover” is used to refer to functionality of a BES Cyber System in a backup and storage regimen. Recommend rewording the requirement to “to restore BES

Cyber System." 2. R1.4: Compliance with R2 should be sufficient. It is very difficult to demonstrate initial verification of this information after the backup. Compliance with R2 should adequately test this process. AEP recommends merging this with R2. 3. R1.5- Preservation efforts may impede the recovery process and reduce reliability as BES Cyber Systems are out of service for an extended period of time while the data is preserved. This seems like a “nice to have” but could be an unnecessary distraction during a stressful time where SMEs should be focused on recovery. Worse still, this could cause double jeopardy with CIP-008. AEP recommends moving this to CIP-008, or making this a guideline. 4. R2.2- This requires that information used in the recovery of BES Cyber Systems stored on backup media be tested once each calendar year. There are no boundaries set on the extent of data required to be tested. Recommend wording in the measures that clarifies that a sampling of information is sufficient.
Yes
Yes
Yes
1. R1.1 While we acknowledge the removal of the term "script" from the requirement, we feel that there should be some clarification of what "custom software" means. We would recommend that the wording be changed to "Any custom application software developed for the entity." 2. R1.1: Could recording software “hashes” be used as an alternative to recording version levels to verify that no unauthorized changes have been made to software on the BES Cyber Asset? AEP recommends this be added to the measures or guidance for this requirement. 3. R1.1.4 should be applicable to systems with external routable connectivity only. 4. R1.1.3: The requirement is not clear in how to determine boundaries on software installed on BES Cyber Assets. Are individual “applications” subject to this? Which “utility applications” are subject to this? Is the version “product level” or “executable level”? Recommend that this requirement at least be addressed in guidance to ensure that “custom software” is neither over or under assessed to meet the requirement. 5. R1.1.4: Please define or provide guidance on “logical network accessible ports”? 6. R1.2: In the measures, "Documentation that the change was performed in accordance with the requirement." To what is the term requirement referring? Recommend removing this item from the measure. 7. R1.3: Using other standards references in the requirement is misleading, time consuming and not in keeping with the intent of a concise security standard. Recommend more use of examples without the reference to the standard numbers. 8. R1.4.1: Remove standards references from the requirement. Provide examples and perhaps add the references to the measures as the source of the data. 9. R3.3: AEP recommends the measure say “of any tools used to perform the assessment” or something similar, since “tools” may not be used in this active vulnerability assessment. 10. R3.4: If security controls tested in the assessment are found to be deficient, would that not be a violation of the CIP standards requirement for that security control? That would require a self report. Could the self report mitigation plan be used as the action plan for 3.4? 11. CIP-010 R1: CIP-007 R1.1 requires a Responsible Entity “..enable only logical network accessible ports…” if they have a High Impact BES Cyber System or Medium Impact BES Cyber System with External Routable Connectivity. For consistency, the applicability of CIP-010 R1 should be changed to High and Medium Impact BES Cyber System with External Routable Connectivity or item 1.1.4 should be removed. (2) R3.1 the specific security controls requirements from CIP-005, CIP-006, and CIP-007 that must be assessed should be defined.
Yes
Yes
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
No
No
(1) The CIP-008 requirements should also be applicable to related EACMS and PACS systems. (2) Part 2.1 permits a paper drill, tabletop exercise, or full operational exercise. Such activity must include a reportable incident scenario. (3) Part 2.1 should require a periodic full operational exercise in the absence of a live, Reportable Cyber Security Incident. Otherwise, Responsible Entities will continue to

only perform a weak tabletop exercise of limited value. (4) Part 2.2 assumes that null deviations need to be documented as well. The requirement language should clearly state that expectation to remove any ambiguity of the expectations placed upon the Responsible Entity. (5) The requirement for lessons learned in Part 3.2 should stipulate that null lessons learned be documented if there were no lessons learned. (6) The High and Severe VSLs for Requirement R3 presumes there must have been lessons learned. The VSLs need to provide for documented occasions where no lessons learned were developed. (7) The guidelines for Part 1.2 defined a Reportable Cyber Security Incident as a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. This definition is too vague and could result in a complete compromise and failure of a BES Cyber Asset not being considered due to available redundant systems being available. (8) The guidelines for R3 properly states that it is possible to have a BES Reportable Cyber Security Incident without any documented lessons learned. The guidance should advise the reader that a null document is still required to demonstrate that an after action review was conducted and no lessons learned were developed.
No
No
No
(1) Part 1.1 needs to define a minimum set of conditions that would require activation of a recovery plan. Otherwise, entities are free to raise the bar to any height, such as only activating the recovery plan in the event of a catastrophic loss of the facility housing the BES Cyber Assets. (2) Requirement R1 needs to make clear that recovery plans for BES Cyber Systems need to contain the necessary steps for restoring the BES Cyber System to a state where it is ready to assume its normal operating role in all respects. The recovery plan is not the same as a Continuity of Operations plan as required by EOP-008. (3) The suggested evidence for Part 1.3 should include documented configuration settings, documented build/restoration procedures, and retention of installation media. (4) The requirement of Part 1.4 is vague and needs clarification. Does verification simply mean a catalog of the backup media demonstrating that the media can be successfully read? Does it mean a comparison of the data recorded on the media against the data that was backed up? Or does it mean a test restoration? (5) Part 2,2 needs to clarify what is meant by the requirement to ensure the information is useable and “is compatible with current system configurations.” (6) Part 2.2 needs to clarify that a test of the information requires either recovery from an actual incident or an operational exercise, either option requiring a system restoration. A tabletop exercise should not be permitted as it will not achieve the intent of the requirement. (7) Requirement R1 needs to clarify the expected level of detail or granularity in the recovery plans. Otherwise, a very generic plan could result in a simple recovery of a minor workstation using a plan also applicable to a complicated SCADA server. (8) The requirement for lessons learned in Part 3.1 should stipulate that null lessons learned be documented if there were no lessons learned. (9) The moderate VSL for Requirement R1 should apply when the recovery plans do not address “one” (not “all”) of the referenced requirements. (10) The High and Severe VSLs for Requirement R3 presumes there must have been lessons learned. The VSLs need to provide for documented occasions where no lessons learned were developed.
No
No
No
(1) Part 1.1.2 should clarify how granular the version identifier should be. Is only the major release level sufficient? Or is minor release level documentation expected? (2) Part 1.1.2 should exclude the anti-malware signature file version identifiers due to the volatility of frequent updates. (3) Part 1.4.1 is likely to result in the Responsible Entity declaring that no Cyber Security Controls are expected to change and thus no testing is required. The purpose of testing is to verify nothing unexpectedly changed and the requirement needs to make that expectation clear. (4) Does Part 1.5.2 permit the documentation of a stand-alone test environment with identified differences from the production environment? Or must the test environment and differences be documented with each change package? (5) Is the assessment required by Part 3.2 in lieu of or in addition to the assessment required by Part 3.1 in the calendar year the Part 3.2 assessment is conducted? (6) Part 3.3 should also apply to Physical Access Control Systems. (7) The High VSL for R1 should apply when the Responsible Entity failed to authorize “one or more” (not “any”) baseline configuration changes. (8)

The phrase “and to document those changes” in the first condition of the High VSL for R1 should be deleted as it is duplicative of the second condition. (9) A VSL condition needs to be defined for R2 for a missed periodicity. (10) The last condition of the Severe VSL for R3 only triggers if all three required elements are missing (due to the use of “and”). A lesser VSL needs to be defined for missing one or two of the three required elements, or the Severe VSL needs to change the “and” to “or.” (11) In the guidance for R3, the passive network discovery should be a review of network connectivity to identify Electronic Access Points. A discovery process cannot presume all access points have already been identified. (12) In the guidance for R3, the passive vulnerability review should include a predecessor step to review the security and configuration policies for the referenced items. Then the review of the actual controls should be conducted to confirm they continue to conform to the policies. (13) In the guidance for R3, the active network discovery should include a physical inspection for those devices that are either incapable of or are configured to not respond to traditional active discovery tools.
No
No
(1) The “methods to identify BES Cyber System Information” requirement in Part 1.1 is vague. Is the required method to determine what information should be considered protected (information characteristic) or is the required method to document that the information is protected (labeling)? (2) The exception found in the first paragraph of Part 2.1 makes no sense and needs to be clarified or stricken. (3) What does “who has possession” mean in the second paragraph of Part 2.1 and in the second paragraph of Part 2.2? Is this an individual? Or would a way bill for a shipment sent by commercial courier be sufficient, even no hand-to-hand chain of custody is maintained? (4) It is not clear if Parts 2.1 and 2.2 permit media to be removed and possibly replaced with clean media, with the Cyber Asset then being redeployed or disposed of while the removed media continues to be maintained until separate erasure or destruction. Parts 2.1 and 2.2 need to track the media and not necessarily the Cyber Asset the media is associated with.
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
In R1, section 1.1.5 indicates a need for baselining security patches. Section 1.3 requires updating documentation of changes to the baseline within 30 days of changes. This would require updating baseline documentation any time security patches are applied. We would recommend striking security patches from this documentation requirement to streamline security updates.
Yes
Yes
Individual
Glen Sutton
ATCO Electric
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Yes
Comment: R2.1 change configuration monitoring presents a significant amount of effort to implement. Specifically the 35 day window does not allow for much flexibility when attempting to perform a manual monthly check of baselines. Additionally, it may not be technically feasible to implement automated baseline monitoring tools within non-standard IT environments where a significant amount of devices and custom applications cannot be monitored with off the shelf products. Consider increasing the 35 day window to 60 or 90 days to provide more flexibility in performing manual baseline comparisons.
Yes
Yes
Individual
Martyn Turner
LCRA Transmission Serivces Corporation
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
In R1, section 1.1.5 indicates a need for baselining security patches. Section 1.3 requires updating documentation of changes to the baseline within 30 days of changes. This would require updating baseline documentation any time security patches are applied. We would recommend striking security patches from this documentation requirement to streamline security updates.
Yes
Yes
Group
Duke Energy
Greg Rowland
No
No
No
(1) Requirement R1.1. “Processes” should be rewritten as “Process(es)” to allow entities flexibility to combine all elements of R1.1 into a single process if they so choose. (2) Requirement R1.4. Duke

recommends removing this requirement in its entirety. Incident handling is assumed to be contained within requirement CIP-008 R1.1 to "respond" to Cyber Security Incidents. (3) Requirement R1.5. Duke recommends that the drafting team coordinate this requirement with the EOP drafting team. This requirement appears to be duplicative to one that appears in EOP-004-2 that could create a spot of double jeopardy in the case of non-compliance. Duke recommends that this requirement only appear in 1 place and suggests that any Cyber Security related requirement should appear only in the CIP standards. (4) Requirement R2.1. Duke recommends that the requirement be rewritten to say, "Test the response plan(s) per CIP-008 R1, at least once every…". The current term "BES Cyber Security Incident response plan" is not a defined term and cannot be assumed to be the ones referenced in R1. (5) Requirement R2.1. Duke asks that the drafting team clarify how many of the response plans, if there are multiple, need to be tested on an annual basis. If the entity creates a dozen response plans, is it the intent of the drafting team that each response plan be tested? Or is testing one response plan per entity sufficient? Would there be justification in testing a sampling of the response plans with a minimum of one? Duke requests that the drafting team provide more clarity. (6) Measure R2.1. Duke recommends striking the reference to "lessons-learned" as they are not specifically required under the requirement. (7) Requirement R2.2. The current language, "Use the incident response plan under Requirement R1" incorrectly assumes that the entity only has 1 response plan developed, when the requirement allows for the development of multiple plans. Duke suggests rewording this to allow for the entity to "Use the applicable incident response plan under Requirement R1". (8) Requirement R2.3. Duke recommends that the drafting team coordinate this requirement with the EOP drafting team. This requirement appears to be duplicative to one that appears in EOP-004-2 that could create a spot of double jeopardy in the case of non-compliance. Duke recommends that this requirement only appear in 1 place and suggests that any Cyber Security related requirement should appear only in the CIP standards. (9) Requirement R3.2. Duke recommends rewording this requirement as follows, "Document any lessons learned associated with a Cyber Security Incident test, per R2.1, or actual incident response to a Reportable Cyber Security Incident, per R2.2, within 30 calendar days after completion of the test or actual incident response.". The insertion of requirement references adds clarity to what is to be documented. (10) Requirement R3.4. Duke suggests striking this requirement in its entirety. The current wording is overly burdensome and would require an update to the plan any time a staffing change occurs. Duke feels that this can be accomplished in the periodic testing of the plan and any updates can be made at that time.

No

No

No

(1) Measure R1.3. Duke recommends that the term "successfully" be striken from the measures section. Duke does not agree with the assumption that merely having the information for recovery available will guarantee successfully recovery of the Cyber Asset. (2) Requirement R1.4. The requirement here to verify backup media "initially after backup" is confusing. This incorrectly assumes that the entity is responsible for creating all backups to backup media. The requirement does not account for the possibility that an OEM may create a backup months or years before delivery of the product that the entity would have no means of testing "initially". Duke requests that the drafting team reword this requirement to only require backup verification when the entity creates the backup. (3) Requirement 1.5. Duke requests that this requirement be reviewed by the drafting team. The current language assumes a cyber event has triggered activation of the recovery plan and therefore the preserving of forensic evidence would be critical. However, the recovery plan may be invoked due to "normal" equipment failure or another type of event in which preserving data/forensic evidence would be unnecessary. Duke suggests that the preservation of data only be required if the recovery plan is triggered due to a Cyber Security incident response plan in CIP-008. (4) Requirement R2.1. Duke asks that the drafting team clarify how many of the recovery plans, if there are multiple, need to be tested on an annual basis. If the entity creates a dozen recovery plans, is it the intent of the drafting team that each recovery plan be tested? Or is testing one recovery plan per entity sufficient? Would there be justification in testing a sampling of the recovery plans with a minimum of one? Duke requests that the drafting team provide more clarity. (5) Requirement R2.2. Duke recommends striking the phrase, "to ensure that the information is useable and is compatible with current system configurations". Duke believes this information is unnecessarily prescriptive and the requirement

should allow the entity the flexibility to use reasonable judgment as to what the test needs to cover. (6) Requirement R3.3. Duke suggests striking this requirement in its entirety. The current wording is overly burdensome and would require an update to the plan any time a staffing change occurs. Duke feels that this can be accomplished in the periodic testing of the plan and any updates can be made at that time. (7) Requirement R3.4. Duke is concerned with the current wording of this requirement. There doesn't seem to be consideration that multiple recovery plans may exist within a single entity. If there are, the requirement is unclear in which plans must be sent to which individuals. The requirement could be misinterpreted to read that any time a single plan changes, all individuals identified in R1.2 must be made aware of the change, even if they are not associated with that specific plan. Duke recommends that the drafting team add additional clarity to the requirement to account for the possibility of multiple plans.

No

No

No

(1) Requirement R1.1. Duke disagrees with the wording of the requirement to apply to "each Cyber Asset indentified, individually or by group" as this is inconsistent with the language in CIP-002 that allows Cyber Assets to be grouped in the beginning of the process into Cyber Systems. Once grouped as a Cyber System, that is how they should be referred to in the remainder of the standards and CIP-010 R1.1 should only apply to applicable Cyber Systems where the requirement may be met at the system level as opposed to the individual Cyber Asset level. (2) Requirement R1.1.1. Duke recommends that the word "exists" be replaced with "is installed". This clarifies that the entity does not have to consider any operating system that could be installed on a Cyber System but may not currently be installed. (3) Requirement R1.1.2. Duke recommends that the word "intentionally" be removed from the requirement. Duke feels that this word is too subjective and could be a compliance issue when one has to demonstrate intent. (4) Requirements R1.1.4 and R1.1.5. Duke is concerned that these requirements are redundant/conflicting with requirements in CIP-007 requiring the entity to manage ports and a patch management program. Duke recommends that requirements related to these controls only appear in one area in the standard and recommend that they be removed from CIP-007 and remain solely within CIP-010. (5) Measure R1.2. Duke recommends that the parenthetical, "performed by the individual or group with the authority to authorize the change" be stricken from the measures section. Duke believes this is unnecessarily prescriptive and doesn't match the requirement as there is no requirement as to who is allowed to make the change. (6) Requirement R1.4.1. Duke recommends removing this sub-sub-requirement in its entirety. Duke does not see the value in determining the controls that could be impacted prior to the change and see the requirement in R1.4.2 as the important step in the process, regardless of what was expected to happen. (7) Requirement R1.4.2. Duke recommends that the drafting team clarify what is meant by "required controls". When referencing entire standards, is it the drafting team's intent that every requirement be re-verified, like a self-audit, when a change is made? Duke requests that instead of using a vague term such as "required controls" that language be inserted to point to specific requirements that must be verified per this requirement. (8) Requirement R1.5.1. Duke recommends that the drafting team clarify what is meant by "required cyber security controls". This language doesn't exactly match that in R1.5, and it is confusing for the entity to determine exactly what should be tested. Duke requests that instead of using a vague term such as "required cyber security controls" that language be inserted to point to specific requirements that must be tested per this requirement. (9) Requirement R1.5.2. Duke believes that the following language should be removed from the sub-sub-requirement, "including a description of the measures used to account for any differences in operation between the test and production environments". Duke does not understand the intent of requiring this type of documentation as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. (10) Requirement R2.1. Duke recommends that the term "continuously" be removed from the requirement. Duke feels that "periodically" captures the intent of an adequate timeframe. There is no reason an entity couldn't employ a continuous monitoring process to go above-and-beyond the standard but the requirement should only spell out the minimum needed to address compliance. (11) Measure R2.1. The current measure says investigation would be needed for any "unauthorized changes" while the requirement calls for monitoring of all changes. Duke suggests that the word unauthorized be added to the requirement such that monitoring is only necessary for unauthorized changes. (12) Requirement R3.1. Duke

recommends that the drafting team clarify what is meant by “cyber security controls”. This language is confusing for the entity to determine exactly what should be tested. Duke requests that instead of using a vague term such as “cyber security controls” that language be inserted to point to specific requirements that must be tested per this requirement. If there is a desire for the drafting team to allow flexibility for the entity to determine what to include in its vulnerability assessment, then all prescriptions should be removed and the language of the requirement could be ended after the words “vulnerability assessment”. (13) Measure R3.1. Duke believes the last phrase in the first bulleted item needs to be removed, “and the individuals who performed the assessment”. This does not align with the requirement and does not provide any value to meeting compliance. (14) Measure R3.1. Duke believes the last phrase in the second bulleted item needs to be removed, “and the output of the tools used to perform the assessment” as this is covered by R3.4 and is not part of the requirement R3.1. (15) Requirement R3.2. Duke believes that the following language should be removed from the requirement, “including a description of the measures used to account for any differences in operation between the test and production environments”. Duke does not understand the intent of requiring this type of documentation as it provides no security benefit and only invites auditors to unnecessarily critique the methods that the entity determines are appropriate to address the differences between the two environments. (16) Measure R3.2. Duke believes that the phrase, “the output of the tools used to perform the assessment” should be removed. This is covered by R3.4 and is not part of the requirement R3.2. (17) Requirement R3.3. Duke is confused by the reference in this requirement to a new Cyber Asset. If a new Cyber Asset is part of an existing Cyber System, then is this requirement applicable? Duke feels that the direction made in CIP-002 should hold true here and a vulnerability assessment would only be required for new Cyber Systems (or those other systems/assets within the applicability section). (18) Requirement R3.3. Duke is confused when there is specific language as to the content of the vulnerability assessment in other sub-requirements of R3 and not within R3.3. Duke recommends that consistency be used and language like that seen in R3.1 be removed to be consistent with the other sub-requirements. (19) Measure R3.3. Duke believes that the phrase, “the output of the tools used to perform the assessment” should be removed. This is covered by R3.3 and is not part of the requirement R3.2. (20) Requirement R3.4. This requirement says to “document the results of the assessments”. Duke is confused as to which assessments require result documentation. Is it the intent that this be all assessments in R3? If so, Duke asks that clarity be added to the requirement to address exactly what needs to be documented here. (21) Requirement R3.4. Duke is concerned with the phrase “remediate or mitigate vulnerabilities identified in the assessments”. Duke has seen regions address this phrase differently and it is not generally understood what the drafting team intends with this statement. Is the intent that identified vulnerabilities do not constitute violations of the requirements that they are found against? If so, Duke requests that the drafting team clearly identify what discovery of vulnerabilities mean and how they are to be addressed in terms of compliance with the other requirements/standards.

No

No

(1) Requirements R1.1 and R1.2. The phrase “and implemented” needs to be removed as it is redundant to the main requirement R1 requiring implementation of the sub-requirements. (2) Requirement R1.2. Duke recommends removing the phrase “including storage, transit, and use” as this is unnecessarily prescriptive. Duke believes the entity should have the flexibility to define their own information protection program and what elements it needs to include based on what is or is not allowed within its own organization. For example, an entity may not authorize transit and therefore requiring a handling process to cover transit would be meaningless. (3) Requirement R1.3. Duke is concerned with the phrase “implement an action plan to remediate deficiencies identified during the assessment”. Duke has seen regions address this phrase differently and it is not generally understood what the drafting team intends with this statement. Is the intent that identified deficiencies do not constitute violations of the requirements that they are found against? If so, Duke requests that the drafting team clearly identify what discovery of deficiencies mean and how they are to be addressed in terms of compliance with the other requirements/standards. (4) Requirement R2.1. Duke recommends rewording the second paragraph of the requirement to the following, “If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsibility entity shall maintain a chain of custody process, which addresses the control of the device while it is outside of a Physical Security Perimeter”. The suggested language change is to demonstrate that the entity may not

always maintain possession of the device and as long as it follows the process, it is meeting compliance with the requirement. (5) Requirement R2.2. Duke recommends rewording the second paragraph of the requirement to the following, “If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsibility entity shall maintain a chain of custody process, which addresses the control of the device while it is outside of a Physical Security Perimeter”. The suggested language change is to demonstrate that the entity may not always maintain possession of the device and as long as it follows the process, it is meeting compliance with the requirement.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
Yes
Yes
Yes
(1) We approve CIP-008 but we support requests clarification follow by NPCC TFIST
Yes
Yes
Yes
(1) We support the comments follow by NPCC TFIST about request clarification
No
No
No
(1) We support comments follow by NPCC TFIST (2)R1.4 :We believe that 1.4 should only apply to Medium impact BES cyber systems with external routable"
Yes
Yes
Group
NRG Energy Companies
Alan Johnson
Yes
Yes
No
1. Requirement R3.2 requires documentation of lessons learned within 30 calendar days after completion of test or actual incident response. This may not allow enough time to complete the investigation and determine appropriate lessons learned. Suggest a change to 60 calendar days. 2. The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents. 3. Requirement R3.3 implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include “as applicable”. 4. Requirement R3.5 – Table 3- identifies possible evidence that can be used to communicate updates of the plan. These suggested media reflects a poor choice of vehicles to communicate these updates to affected personnel due to the confidentiality of the material.
No
Yes
No
Requirement R3.4 – Table 3- identifies possible evidence that can be used to communicate updates of

the plan. These suggested media reflects a poor choice of vehicles to communicate these updates to affected personnel due to the confidentiality of the material.
In Requirement R3.3, 30 days should be extended to 60 calendar days to make the overall timing for the activities in R3 more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan.
No
No
No
1. Revise Requirement R1.3 from a 30 day timeline to 90 days (or removed) to allow for sufficient time to process/document the required changes and verifications. The 35-day timeline in Requirement R2.1 should be extended to 90 days to allow for a quarterly review process. 2. The applicability of CIP-010-1 R3.1 and R3.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports the proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity. Oncor 3. In requirement R3, please clarify whether an external vendor needs to perform the annual Vulnerability Assessment or can the Responsible Entity perform the task reviewed by its Internal Audit group. 4. Additionally R1.4.1 and R3 specifies that CIP-006-5 controls need to be included in the Vulnerability Assessment. As this is a substantial change from the prior definition of CVA, can guidance be provided for this assessment?
No
Yes
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
R3.1 & R3.3 - The Requirement to perform Vulnerability testing and documentation for Medium Impact cyber assets outside of a control center should be deleted. In a field environment, where individual assets may number in the hundreds, and where the potential impact is typically much less, the effort is not only problematic but has the potential to reduce, not improve reliability. R3.3 & R3.4 - Why R3.3 does not include Medium Impact BES Cyber Systems while R3.4 does. Until the bright-line criteria have been assessed against the company assets, it is difficult to determine the impact this will have on Medium Impact BES Cyber Systems.
Yes
Yes
R2.2 – Please clarify “chain of custody”.
Individual
Kayleigh Wilkerson
Lincoln Electric System

Yes
Yes
Yes
No
No
Yes
No
No
No
[R1] Outside of PCs and protective relays, LES does not believe there is a need to collect the information in CIP-010 R1. This Requirement should only apply to a subset of cyber assets like PCs and protective relays.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information.
Individual
Joe Petaski
Manitoba Hydro
In R2.1, it is unclear what makes an operational exercise to be deemed as “full”. We suggest changing “with a full operational exercise” to “with an operational exercise”.
R2.1: The “chain of custody” documentation is too onerous for many situations (including moving cyber assets from one PSP room to another!). we suggest rewording: “Or alternatively, the responsible entity shall have procedural controls to ensure the BES Cyber System Information remains at all times in the possession of personnel who are authorized for access to the BES Cyber System Information.”
Individual
Michael Schiavone
Niagara Mohawk (dba National Grid)
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Group
Arizona Public Service Company
Janet Smith
Yes
Yes
Yes
Yes
Yes
No
AZPS recommends that the table 1.4 Requirements should read "Verify that backups of information essential to recovery complete successfully.”
AZPS recommends changing the word “Distribute” in the table 3.4 Requirement to “Communicate”. AZPS believe the plans are CIP Confidential Information that may be best communicated via a link to the updated plan to ensure only those with authorization are able to access the document.
Yes
Yes
Yes
Yes
Yes
Individual
Michael Jones
National Grid
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Jonathan Appelbaum

The united illuminating Company
Yes
Yes
Yes
UI concurs with EEi Consensus comments.In a addition, for R 2 we are concerned with plural in plan(s). A Registered Entity may have one plan that explains response to different types of incidents. It should be clear that only one Test of the plan is required, as opposed to testing every incident response tree.
Yes
Yes
Yes
UI agrees with EEI consensus comments
UI agrees with EEI consensus comments
No
No
No
UI agrees with EEI consensus comments
Yes
No
UI agrees with EEI consensus comments
Individual
Alice Ireland
Xcel Energy
No
Yes
Yes
Regarding CIP-008-5 R1: Regarding the definition of reportable cyber security incident: CIP-008-5 R1 points to EOP-004-2 for the definition of a reportable cyber security incident. EOP-004-2 points back to CIP-008-5 for the reporting criteria. The reference to EOP-004-2 seems unnecessary. The CIP v5 definitions define a reporting cyber security incident as, “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.” This definition is much broader than the definition of cyber security incident. “Reliability tasks” is undefined as is “compromised or disrupted.”
Yes
Yes
No
We suggest that R3.2, 3.3, and 3.4 be deleted and R3.1 replaced with the following language: “For any required change to the recovery plan (due to deficiencies or lessons learned from recovery plan tests or actual incident recoveries, or changes in roles, responsibilities, or technology), update the recovery plan and distribute updates to each individual responsible under R1.2 within 60 calendar days.”
Yes
Yes
Yes
No
No
1) R1.1 introduces less flexibility by implying that we need to have a classification (or at least labeling scheme) for ‘BES Cyber Systems Information’ rather than allowing us to classify and handle the same way we classify and handle other types of corporate information. Recommend removing from

Evidence the reference to labeling. 2) R1.2 there is no definition of ‘use’ of information. How is that different from access (which is handled in a different standard), labeling (covered in R1.1), and release to authorized others (covered in ‘transit’ and access). Recommend removing the word ‘use’ from the requirement. 3) R2.2 is unclear if scope is the storage media within the Cyber Asset (2.1) or if it also includes backup media. It just says storage media which can mean many things. Please clarify. 4) R2.2 please clarify ‘chain of custody’ documentation requirements. Is that simply the name of the person and the start/end time of possession. 5) R2.1 redeployment/reuse and 2.2 disposal are very similar in language, consider consolidating into a single requirement.
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
Yes
Yes
Yes
Yes
No
Yes
Regarding R2.2 which states: “Test information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is useable and is compatible with current system configurations”. BPA believes this requirement could be interpreted to mean that the entity is required to recover the data to a functionally equivalent system and operate the system to determine whether the data is usable or not. In the security and IT industry, it is understood that the purpose of testing backups is to determine whether the data that you thought you backed up was actually backed up, and is recoverable from the media. First, when the data is initially stored on the backup media, it is verified to ensure successful backup. Later, when the backup is tested, it is typically accomplished by reading the data on the backup media to determine if the media is still readable. It is BPA’s interpretation that the new standard as written appears to compel entities to perform operational testing on a functionally equivalent system to validate the usability of the data rather than performing a restoration to validate the viability of the data. BPA recommends the following rewrite to clarify that the intent of the requirement is to validate the viability of the backup media: “Test Backup Media containing information used in the recovery of BES Cyber Systems at least once each calendar year,

not to exceed 15 calendar months between tests, to ensure that the information is usable and is compatible with current system configurations". Regarding Table R2.2 Measures: BPA believes the language of the Measures should be revised to align with the language that was removed from the requirement. BPA recommends: "Evidence may include and is not limited to, dated evidence of a test of information used in the recovery of a BES Cyber System that is stored on backup media at least once each calendar year, not to exceed 15 calendar months between tests, to ensure that the information is usable and is compatible with current system configurations: Regarding R2.2, BPA believes the entity needs to test the backup media and the Measures in Table 2 need to reflect the same language.
Yes
No
Yes
While BPA agrees with the goal in R2.1 of automated monitoring of baseline configuration changes, BPA believes a 35 day requirement is far too aggressive to accomplish on some Cyber Assets where automated monitoring is not possible and given the large number of devices BPA has that will need to be manually monitored for changes. For these cyber assets, BPA suggests an annual review period is more feasible as it will be in line with normal periodic maintenance cycles. As discussed in the Guidelines, for some cyber assets it is not technically possible to implement automated monitoring due to the capabilities of the device. For other cyber assets, while it may be technically possible to monitor, the inability to integrate with a centralized automatic monitoring system (e.g. Tripwire) without significant system and/or network changes is problematic. This will likely expose the cyber asset to additional cyber security risks if added to a primary network just for monitoring purposes, hence reducing overall security and reliability. For cyber assets such as a terminal servers used for SCADA RTU serial communication, the risk of inadvertent or unauthorized changes is minimized by other compensating measures, including and not limited to, isolation on small private networks. Even if manual monitoring is acceptable in this situation, it has the potential to introduce additional risk of inadvertent accidental changes due to an increase in frequency of human interaction with the device that will need to be completed to perform the required monitoring. Additionally, the explanation provided in the Guidelines for this requirement about the acceptability of using a manual process is not clear regarding when technical feasibility exception will be allowed. BPA believes the explanation needs to be clarified. An example would be very helpful. Suggested Changes: BPA would like to see this requirement implemented for devices that can accomplish it automatically. All devices that cannot implement this requirement automatically should be allowed a technical feasibility exception. The proposed change to requirement 2.1 is as follows: Where technically feasible, automatically monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1), and document and investigate detected unauthorized changes. BPA agrees with the intent of the CIP-010 guidelines and can vote vote yes on the standard should the drafting team address BPA's concerns regarding requirement 2.1. For BPA to have an affirmative position for this standard, CIP-010 R2.2 language needs to be revised to the following: "Where technically feasible, automatically monitor changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1), and document and investigate detected unauthorized changes". If the SDT does not agree with the removal of manual, periodic monitoring, than at a minimum, BPA suggests extending the monitoring period of 35 calendar days to annual monitoring.
Yes
Yes
Individual
Benjamin Beberness
Snohomish County PUD
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Yes
CIP-011-1 R1 The draft CIP versions 5 Reliability Standards are very BES definition centric. Due to the proposed changes to the BES definition it is very difficult for the electric industry to comment on a standard as it is unclear if the currently or proposed BES definition will be applied. This change in the definition could significantly change the applicability of the version CIP Reliability Standards. Although it is clear the SDT has made attempts to size the applicability of the CIP version 5 requirements with the size of the registered entity, the current draft will cause significant resource burdens on facilities that have demonstrated they cannot impact the reliability of the Bulk Electric System. As a Transmission Dependent Utility SNPD supports a reliable system because we are at the end of the system and SNPD's customers are exposed to all disturbances on the main grid. However SNPD also support efficiency and spending significant resources with little to benefit is not beneficial to the reliability of the BES or to the Level of Service ("LOS") SNPD provides its customers.
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
Yes
No
1.) PPL Affiliates appreciate all the value-added work the SDT has provided on the CIP Version 5 project. PPL Affiliates would like the SDT to consider changing CIP-008 R3.2 to include language for consistency with the ERO Event Analysis Process. • PPL Affiliates submit for consideration the following language... 'Document any lessons learned associated with a Cyber Security Incident test incident response within 30 calendar days after completion of the test incident response. Document any lessons learned associate with an actual Reportable Cyber Security Incident per the ERO Event Analysis Process Appendix E when the Cyber Security Incident results in an event on Appendix E. If the Cyber Security Incident did not result in an ERO Event Analysis per Appendix E, the lessons learned shall be performed within 30 calendar days.' • PPL Affiliates believe that the consistency of reporting requirements for the lessons learned eases the training and compliance requirements without any adverse impact on reliability
No
Yes
No
R3.1/R3.2: Requirement to document lessons learned and update recovery plans accordingly within 30 days, though feasible following an exercise, would likely be too prescriptive following an actual recovery. This is due to the time required to effectively evaluate the circumstances and response to an actual recovery (especially a major event). 90 days or longer would be more appropriate in such an instance.
R1.4: It seems that "…verified initially after backup…" is confusing to many. If the intent is to run a verification pass on the backup media to assure that this matches the source (an automated function with most backup software), then this should be made clearer. If the intent is simply to verify a successful backup occurred (as per the Measures), then this should be made clear.
Yes
Yes
Yes

Yes
Yes
Individual
Larry Watt
Lakeland Electric
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
No
No
No
Tampa Electric is in support of the comments from EEI for CIP-008-5
No
No
No
Tampa Electric is in support of the comments from EEI for CIP-009-5 R3
Tampa Electric is in support of the comments from EEI for CIP-009-5
No
No
No
Tampa Electric suggests that it is not clear if this means a vulnerability assessment is required for every cyber asset or a sampling of cyber assets. As this relates to relays, it seems like once a set of cyber security controls are in place and tested to be adequate then a review of those controls at a single location would be adequate if the same controls are used everywhere. As more equipment gets pulled into scope doing annual reviews such as required here will become increasingly onerous. For R1.2, Tampa Electric recommends that applicability be changed to High Impact BES Cyber Systems only. In addition, there is ambiguity in the phrase “Documentation that the change was performed in accordance with the requirement.” For R1.3, Tampa Electric suggests 90-calendar days due to outside vendor responses needed. For R1.4, Tampa Electric suggests that the legacy CIP-007 R1 language should be used. We also request clarification on R1.4.2: What is considered BES Cyber System “availability” – if one component has an issue is that the entire system? Should availability read “reliability”? For R 2.1, Tampa Electric suggests the SDT modify requirements language to be more consistent with updated R1, which is to get rid of the baseline language. Please provide clarification

on what is considered the “record of investigation?” Also, if no change is detected during a monitoring period, how does an entity demonstrate “no change”? For R3.1, Tampa Electric recommends that the SDT add “externally routable” to Medium Impact, Associated Protected Cyber Assets. We would also like clarification for the following question: Does this requirement mean each system individually has to be assessed or does grouping of the same technology qualify?
Yes
No
Tampa Electric agrees with the comments submitted by EEI. In addition, we note that the Rationale for R1 is incomplete, stopping in mid-sentence. For CIP-011-1 R2.1, Tampa Electric would like to raise a concern related to hardware failures for systems where the entity is under contract with a third party company that owns the hardware and software. If the failed equipment must be returned to that company under the terms of the contract, there appears to be no way to destroy the information. For restoration of functionality, it may not be under the entity’s direct control to be able to track and document all hand-offs of equipment to restore service. For CIP-011-1 R2.2, Tampa Electric suggests the same concern raised in R2.1. In addition, outsourcing arrangements may prevent the documentation of all hand-offs of information and tracking that information through disposal.
Individual
David R. Rivera
New York Power Authority
No
No
No
NYPA agrees with NPCC comments
No
No
No
In R1 Part 1.5, the reference to forensics should not be part of the CIP-009 Standard.
No
No
NYPA agrees with NPCC comments, plus - NYPA would like to emphasize the suggestion of returning to the Draft 1 text.
Yes
No
NYPA agrees with NPCC comments.
Individual
Annette Johnston
MidAmerican Energy Company
No
No
No
(1) CIP-008 APPLICABILITIES: Add the qualifier “with External Routable Connectivity” to all of the medium impact BES Cyber System applicability listings in CIP-008, to ensure consistency between the standards. Some requirements of other standards (CIP-005, -006, -007) that “feed into” CIP-008 include this qualifier. For example, CIP-006 does not require monitoring for dial-up BES Cyber Systems, so it would be difficult for dial-up systems to meet the CIP-008 requirements. (2) CIP-008 GUIDELINES: We recommend references to the DHS and NIST documents be deleted, since NERC does not track those documents to determine if they remain consistent with the NERC standards. It would be more appropriate to include references to NERC documents, such as the Security Guideline: Threat and Incident Reporting, if NERC plans to continue to maintain this document. (3) CIP-008 R1 REQUIREMENT: (a) R1.1: No comments. (b) R1.2: MidAmerican Energy has provided comments on the definition of Reportable Cyber Security Incident to eliminate the term “reliability tasks,” since this

term is not defined or explained. While the SDT notes in the consideration of comments that they are continuing to coordinate with Project 2009-01, we still believe that CIP-008-5 should be written to "stand on its own" in the event CIP version 5 becomes effective before EOP-004-2. CIP-008-3 required a process for reporting to ES-ISAC. We propose revising R1.2 to ensure CIP-008-5 includes processes to report. Proposed text: "Processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and to report." (c) R1.3: No comments. (d) R1.4: No comments. (e) R1.5: No comments. (4) CIP-008 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. See rationale in comment form D question 17 and comment form A question 4 comments 12, 16, 17 and 18. (b) R2.1: ANNUAL: Revise "at least once each calendar year, not to exceed 15 calendar months between executions," to "once each calendar year or a period not to exceed 15 calendar months between executions." Rationale: see comment form D question 17. (c) R2.2: Delete this part, since the R2 statement above the table already states the entity "shall implement the plan" (use the plan). In addition, the statement "Document deviations from the plan" is duplicative of R3.2, which requires documentation of lessons learned. During an actual incident, there may not be time to document deviations "during the response." These deviations might be documented after the response, but they would be covered in R3.2 as lessons learned. (d) R2.3: Delete this part, since evidence retention is already covered in C.1.2. If this is retained, the word "relevant" should be deleted. (5) CIP-008 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (6) CIP-008 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: This requirement is duplicative with R2.1 and presents double jeopardy. R3.1 should be deleted. (c) R3.2-R3.5: In its CIP-008 consideration of comments, the SDT quoted paragraphs from Order 706 that were not CIP-008 directives (P651-CIP-007; P728-CIP-009; P731-CIP-009). The only FERC directive for CIP-008 was paragraph 686, which directed revisions to address lessons learned. While we support making timely updates to the Cyber Security Incident response plan, we believe R3.1-R3.5 has significantly increased the documentation burden associated with CIP-008 requirements due to the tracking of multiple dates. In paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to plans are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of R3.2-R3.5 into one part to ensure lessons learned, updates to the plan and communications are completed within the 90 days achieves FERC 706 but is less prescriptive and less of a documentation burden. Examples of changes that would require updates to the plan in R3.4 can be moved to guidelines. Following is proposed text: R3.1: "Update the Cyber Security Incident response plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned." (d) R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Examples: 1) revised response plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates." CIP-008 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
No
(1) CIP-009 R1 REQUIREMENT: (a) R1.1: No comments. (b) R1.2: No comments. (c) R1.3: Change

"BES Cyber System" to "applicable Cyber Assets" in the requirement, since it applies to more than just BES Cyber Systems. FERC 706 had two different directives in paragraphs 739 and 748, which are listed in the change description with CIP-009 R1.4. We think paragraph 748 would be better addressed by adding a phrase to R1.3. The directive is to have procedures to ensure verification that backups are successful. Since R1.3 is to have processes, we think the following revised text would address paragraph 748: "One or more processes for the backup and storage of information required to recover applicable Cyber Asset functionality. Processes should include verification that backups are successful and backup failures are addressed so that backups are available for future use." (d) R1.4: By addressing Order 706, paragraph 748 in R1.3, we think R1.4 should be revised to be focused on paragraphs 732-739. We do not support the draft 2 text that includes the term "initially," since this would be a significant administrative burden that goes beyond the FERC directive. In paragraph 739, FERC directs the ERO to incorporate guidance, so we think the directive could be met with guidance. However, we would support the new requirement if the scope is revised to better reflect the directive in these paragraphs. In paragraph 739, FERC refers to "significant changes made to the operational control system." FERC did not express concern about Physical Access Control Systems or Electronic Access Control or Monitoring Systems. We suggest these be deleted from the applicability. We propose the following revised text to better reflect FERC's concern with significant changes: "Information essential to BES Cyber System recovery that is stored on backup media shall be verified after a significant change to the hardware or software to ensure that the backup process completed successfully." We suggest a 90 day evidence retention on this new requirement. R1.4 is not listed in the implementation plan. With our revised text, it would not need to be included in the implementation plan. (e) R1.5: While we think draft 2 has addressed some of our concerns with draft 1, changes made to the definition of CIP Exceptional Circumstance introduce some new issues. In most cases when the recovery plan is invoked, there will be a hardware, software or equipment failure. The revised definition of CIP Exceptional Circumstance includes "an imminent or existing hardware, software, or equipment failure." Under draft 2, CIP-009 R1.5 would never be required because of the addition of CIP Exceptional Circumstances to R1.5 and the addition of hardware, software or equipment failures to the definition. We propose the following text that would eliminate this issue but still meet the FERC directive in paragraph 706: "Processes to preserve data necessary to determine the cause of a BES Cyber Incident that triggers activation of the recovery plan(s), within capabilities of the device or operational requirements. Data preservation should not impede or restrict system restoration." Limit the applicability for this new requirement to high impact BES Cyber Systems and medium impact BES Cyber Systems at control centers. (2) CIP-009 R1 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (3) CIP-009 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R2.1: ANNUAL: Revise "at least once each calendar year, not to exceed 15 calendar months between tests," to "once each calendar year or a period not to exceed 15 calendar months between tests." APPLICABILITY: The applicability is limited to high impact and medium impact at control centers, along with their associated EACs and PACs. This means testing for substations and generating plants that are not high is not included. Was this the intent of the SDT? (c) R2.2: ANNUAL: Revise "at least once each calendar year, not to exceed 15 calendar months between tests," to "once each calendar year or a period not to exceed 15 calendar months between tests." (d) REQUIREMENT TEXT: We continue to have concerns with the addition of the phrase "is compatible with current systems." An entity will need significantly more documentation associated with the tests in order to show auditors that the backup media was "compatible with current systems." The FERC directives in paragraphs 739 and 748 state that auditors should be able to look at a responsible entity's policies, procedures and records to determine how the testing is done and what recent tests have been performed." We do not believe the FERC directive requires the additional phrase. We also suggest adding a phrase that would eliminate the possibility of double jeopardy with EOP-008. Here is proposed revised text to address both concerns: "Unless covered by EOP-008, test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media at least once each calendar year, or a period not to exceed 15 calendar months between tests, to verify the backup media is operational and the information is useable." (e)MEASURES AND CHANGE DESCRIPTION: Remove references to "initially." (f) R2.3: Add a phrase that eliminates the possibility of double jeopardy with EOP-008: "Unless covered by EOP-008, test …." and add "representative sample of." (4) CIP-009 R2 VSLs:

Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (5) R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. (c) R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Examples: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates." (5) R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities." (6) CIP-009 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
No
No
No
(1) CIP-010 R1 REQUIREMENT: MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (a) R1.1 APPLICABILITY: MidAmerican Energy proposes limiting this documentation-laden requirement to high impact. If that is not possible add "with external routable connectivity" to medium impact. Version 4 did not apply to noncritical. (b) R1.1 REQUIREMENT: MidAmerican Energy proposes changing this requirement to a program or performance based level to allow the entity more flexibility with configuration change management, eliminate proposed duplication with other requirements and prevent the addition of unnecessary documentation burden. For example, what is prescribed precludes entities from using a program like Tripwire, which does automated file to file comparisons to look for and report changes. Also, there are several instances in the proposed requirement that increase the risk for double jeopardy by duplicating other requirements. For example: 1.1.1, 1.1.2 and 1.1.3 are covered in CIP-009 R1.3; 1.1.4 is covered in CIP-007 R1.1; and 1.1.5 is covered in CIP-007 R2.3. In the FERC FFT order (docket RC11-6-000) paragraph 81, FERC invites NERC to gain efficiencies and minimize compliance backlogs by removing "requirements that likely provide little protection for Bulk-Power System reliability or may be redundant." Requirement 1.1.4 would require the industry to account for more than a billion ports if each of 214 entities had less than 100 routable assets. Requirement 1.1.5 would require an entity to document tens of thousands of unique patch installs for less than 200 Windows based Cyber Assets. (c) R1.2 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (d) R1.2 REQUIREMENT Proposed text: "Authorize changes to: security controls, operating systems, application software versions, custom software, ports or patches. Authorize changes to add or remove hardware." This addresses the SDT's intention to explicitly authorize changes. (e) R1.3 APPLICABILTY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (f) R1.3 REQUIREMENT: The change rationale for

this requirement states it is equivalent to the previous versions (CIP-007 R9 and CIP-005 R5); however, we think this V5 requirement significantly expands the scope of the documentation burden beyond the earlier versions, beyond what FERC has directed and beyond what is needed to ensure security of the grid. FERC's concern with up-to-date documentation is stated in paragraph 651 of Order 706 in the CIP-007 section: "The Commission believes that having correct documentation of methods, processes and procedures for securing a responsible entity's system is necessary because if an event occurred before documentation was updated, an operator may not know of a change and could operate the system using out of date information." Version 1 of CIP-007 required 90 days. In response to Order 706, version 2 was revised to 30 days for CIP-007 – meeting the directive. MidAmerican Energy also has concerns about possible triple jeopardy with the references to CIP-005 and CIP-007. Because FERC's concern is included in the CIP-007 section of Order 706 and the systems security controls are included in CIP-007-5, it may be better to move this requirement to CIP-007 and CIP-005 as a requirement to update and designate what documentation in the respective standards requires updates within what timeframe. (g) R1.4 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact. (h) R1.4 REQUIREMENT: MidAmerican Energy is concerned about scope expansion with the term "BES Cyber System availability". Delete this phrase. For example, does this mean there is a violation if you do a re-boot after a patch installation and the system is down momentarily (and is therefore "unavailable") during the re-boot? Current v4 and VSLs do not indicate this. Also, change the word "determined" to "identified". Absolute assurances are not required; see FERC Order 706 paragraph 399. (i) R1.5 (1.5.1) REQUIREMENT: MidAmerican Energy proposes deleting "that models the baseline configuration to ensure that required cyber security controls are not adversely affected." This is redundant to the concept in the last sentence, which requires documenting differences between test and production when a test environment is used. (2) CIP-010 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-010 R2 REQUIREMENT: MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. 1) R2.1 APPLICABILITY: Remove Associated Physical Access Control Systems and Associated Electronic Access Control and Monitoring Systems and Associated Protected Cyber Assets. This is a new requirement and appropriate to the risks for high impact. 2) R2.1 REQUIREMENT: "Where technically feasible, monitor at least every 35 days for unauthorized changes. Document and investigated detected unauthorized changes." Adding "unauthorized changes." Double jeopardy exists for this requirement with R1. Move the requirement to R1. If a paperwork error occurs in authorizing a change and this requirement uncovers it, this should be addressed under R1, not a separate R. (4) CIP-010 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (5) CIP-010 R3 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: ANNUAL: Revise "at least once each calendar year, not to exceed 15 calendar months between assessments," to "once each calendar year or a period not to exceed 15 calendar months between assessments." (c) R3.1 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity" to medium impact and associated protected cyber assets. (d) R3.1 REQUIREMENT: Remove references to other CIP standards because it creates risk of double jeopardy. (e) R3.2 REQUIREMENT: MidAmerican Energy proposes ending this requirement after the words, "…that minimizes adverse effects)." Delete "that models the baseline configuration of the BES Cyber System in production." This is redundant to the concept in the last sentence which requires documenting differences between test and production when a test environment is used. (f) R3.3 REQUIREMENT: MidAmerican Energy proposes to change the words "prior to adding" (which is prior to being in scope) to "before closing the change." The Cyber Asset is not a new BES Cyber Asset until it has been installed. Some vulnerability assessments actions only add value to assess after connected to the ESP as part of implementation and post implementation testing. Also, move the parenthetical explanation of a like replacement to guidance. (g) R3.4 APPLICABILITY: MidAmerican Energy proposes adding "with external routable connectivity"

to medium impact and associated protected cyber assets. (h) R3.4 REQUIREMENT: Simplify wording of requirement to minimize documentation and focus on the cyber security related outcome. MidAmerican Energy proposed text: “Document identified vulnerabilities. Establish and implement plans for mitigation or remediation of identified vulnerabilities.” (6) CIP-010 R3 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (7) CIP-010 R3 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.
No
No
(1) CIP-011 R1 REQUIREMENT: 1) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (a) R1.1: The R1 statement requires “implementing.” “Documentation” is for evidence. Text: “One or more methods to identify BES Cyber System Information.” (b) R1.2: No comments. (c) R1.3: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between assessments,” to “once each calendar year or a period not to exceed 15 calendar months between assessments.” (2) CIP-011 R1 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention. (3) CIP-011 R1 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (4) CIP-011 R2 REQUIREMENT: (a) MidAmerican Energy proposes adding the following to the R statement above the table: Each Responsible Entity shall: implement; measure performance to detect flaws; correct detected flaws expeditiously; and take corrective action, if needed, that may prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R2.1 and R2.2: The applicability includes dial-up medium impact BES Cyber Systems. The second paragraph in this requirement is contradictory with the applicability, since it references PSPs and dial-up assets do not have to be in a PSP. (c) We do not support the requirement for chain of custody. This is a legal term that requires significant administrative and documentation burden. (d) Order 706 paragraph 631 states “the requirement ultimately needs to assure that there is no opportunity for unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it.” Paragraph 633 in the determination states “clarify what it means to prevent unauthorized retrieval of data from a cyber asset prior to discarding it or redeploying it” and notes there is a difference between redeploying and discarding. Guidance is a place to clarify. However, the last sentence of guidance in draft two should consider adding “purge” as an option along with “clear.” The proposed parenthetical in R2.1 also provides some clarity. Note: We would also propose adding information to guidelines regarding “out of control of the entity or its contractors.” If an entity has shipped an asset to an outside vendor to do the destruction or sanitization or to conduct analysis of a failed Cyber Asset, a secured shipper would be considered secure for handling purposes. (e) Because of these issues, we propose R2.1 and R2.2 be combined and added to the table for R1 where R1.2 requires handling procedures for BES Cyber System Information. This reduces double jeopardy. Start the text with: “Prior to the disposal or applicable Cyber Assets that contain BES Cyber Information or to the reuse of” (f) The second paragraph of R2.1 should be deleted as redundant to handling required in R1.2. (g) Add “for reuse” after “except” in the parenthetical in R2.1. (i) If it’s necessary to keep the content of the second paragraph of R2.2, we suggest it be incorporated into R1.2, since it relates to information handling and transit. Text such as: “One or more documented and implemented procedures for handling BES Cyber System Information during storage, transit and use, as well as, procedures for preventing unauthorized retrieval when an applicable Cyber Asset is removed from the Physical Security Perimeter before action is taken to prevent unauthorized retrieval from the data storage media.” (5) CIP-011 R2 VSLs: Corresponding to the proposed revision to the requirement statement, the VSLs should be revised to: severe-not implemented, higher-not measuring to detect, moderate-not correcting detected flaws, lower-not considering prevention.
Group
MRO NSRF
Will SMith
Yes

No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards. We do not believe that they have fully resolved these issues. [R2.2] – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. [R 3.1] – Suggest strike "and update" to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage "update, if necessary." [R3.5] – Suggest striking "distribute". What constitutes distribution? Suggest retaining "notification" approach. Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals
No
No
Yes
The MRO NSRF believes that the level of descriptiveness and compliance thereof, woudl be disruptive and prohibitive. [R1] – The standard isn't clear whether the recovery plans are for recovery of the asset, system, or function? Please clarify. [R1.4] – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes "initial," "verification," or "ensure the process completed successfully"? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: "Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function." [R1.5] – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: "Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s)." [R2.1] - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a "full operational exercise" on all systems, or is a representative sampling sufficient? [R2.2] – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. [R2.3] – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a "standby" system for testing. [R3.4] – Once again the use of the word "distribution". If I notified a vendor of an update to the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its "distribution".
No
No
No
[R1.1.3] – Proposed verbiage: "Any custom compiled software". [R1.4] – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. [R2.1] – Recommend replacing "technically feasible" with "Within the capabilities of the system or network configuration." Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or

quarterly verification, because a manual process of verifying the baseline will be administratively burdensome. [R3] – What is the definition of an “active vulnerability assessment”? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an “active vulnerability assessment” on all systems, or is a representative sampling sufficient? Recommend striking “CIP-006” from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts
Individual
Richard Salgo
NV Energy
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
We note that in R1, part 1.4.2, the verification that controls are not adversely affected is to occur “following the change”, but there is no specification as to how long an entity may take to make this verification. This appears to be a weakness, and we presume that an auditor will attempt to pass judgment on an entity’s promptness of verification.
Yes
Yes
Group
NESCOR/NESCO
Annabelle Lee
No
No
R1: Incident Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com/ General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library Part 2.2: Part 2.2 does not address new vulnerabilities or threats. Consider adding a requirement that the plan be revised based on new threats/vulnerabilities. As stated, "Retain relevant documentation related to Reportable

BES Cyber Security Incidents for three calendar years." Is this sufficient for law enforcement, state, and federal requirements? Also, if the documentation is in electronic form, consider storing it in encrypted form and signed to ensure confidentiality, non-repudiation, and integrity. As stated, "Review each BES Cyber Security Incident response plan for accuracy and completeness initially upon the effective date of the standard and at least once each calendar year thereafter, not to exceed 15 calendar months between reviews, and update if necessary." Consider revising the plan if there are incidents, new vulnerabilities, new threats, and modified security configurations. As stated, "Review the results of BES Cyber Security Incident Response Plan(s) test or actual incident response within thirty calendar days of the execution, documenting any lessons learned associated with the response plan." Consider modifying other relevant documentation, e.g., configuration management plan, access control policies, audit policies, etc.
No
Yes
R1.3: For Part 1.4, what does “verified initially” mean? Each time the backup runs, or the first time after the asset was commissioned? (Could be years ago). If the latter, evidence retention might be an issue for long-life assets. As stated, "Conditions for activation of the recovery plan(s)." The terms “response plans” and “recovery plans” are not adequately defined. It is not clear what the differences are between the two types of plans. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.4: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures. R3.2: For an actual incident recovery, consider requiring that the data produced in R1.5 be assessed in reviewing the recovery process. This might be included in the requirement, in the measures, or both. R3.4: NERC could consider updating the Measures in Part 3.5 of CIP-009-5 Table R3 to ensure communication of update activities be conducted in a manner that requires an irrefutable acknowledgment on the part of the receiver of the communication. As stated, "Review the results of each recovery plan test or actual incident recovery within thirty calendar days of the completion of the exercise, documenting any identified deficiencies or lessons learned." and "Update the recovery plan(s) based on any documented deficiencies or lessons learned within thirty calendar days of the review required in Requirement R3, Part 3.2." These plans may require changes to other applicable plans, procedures, and documentation, e.g., configuration management documentation, security configurations, access control policies and procedures.
No
No
No
R1.1: As stated, "Develop a baseline configuration of the BES Cyber System, which shall include the following for each BES Cyber Asset identified, individually or by specified grouping: 1.1.1. Physical location; 1.1.2. Operating system(s) (including version); 1.1.3. Any commercially available application software (including version) intentionally installed on the BES Cyber Asset; 1.1.4. Any custom software and scripts developed for the entity; 1.1.5. Any logical network accessible ports; and 1.1.6. Any security-patch levels." This is not a comprehensive list of what could be included for each cyber asset. It is not clear how this list applies if the device is hardware only. Also consider adding communication protocols. NERC could consider adding a requirement to include in the baseline any non-standard configurations of the BIOS, operating system, services, etc. For example, BIOS version, BIOS boot disk order, BIOS password, changes to Windows registry entries, changes to service/task scheduling priorities, addition of periodic processes via modifications of tools like crontab, etc. NERC could consider adding a requirement to explicitly include in the baseline any remote access services, eg. RDP, VNC, PCanywhere, etc. NERC could consider adding programmable device load versioning to

the list of items in the configuration baseline. This should include any executable or loadable image that can be modified without requiring physical access to BES Cyber System component internals. Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R2: Configuration Management could include industry best practices, which are documented in the IT Infrastructure Library (ITIL) - http://www.itil-officialsite.com General descriptions are in Wikipedia - http://en.wikipedia.org/wiki/Information_Technology_Infrastructure_Library R3: There are no requirements that an entity identify or document third party connections to BES Cyber Assets. Such connections are common and a high source of potential risk. NERC could consider developing requirements to identify and document third party connections, and authenticate and control access, both ephemeral (remote access) and persistent, from such connections. Furthermore, any and all requirements specified by the CIPs for the BES Cyber Assets accessed, including technical controls, policies, background checks, information handling, etc., should also apply to the third party systems. R3.2: R3.2 calls for vulnerability assessments every three years. CIP 007-3 R8 requires vulnerability assessments annually. No rationale is given for weakening this requirement. As of January 2 2012, the National Vulnerability Database contains 49053 CVE vulnerabilities, with 11 being added per day. Even without likely acceleration of this growth rate, this implies 4000 new vulnerabilities will be discovered each year. Even if only a small percentage of these apply to BES cyber assets, this could mean a significant number of KNOWN vulnerabilities in BES cyber assets by the time a vulnerability assessment comes due. Because of the constant change and introduction of new vulnerabilities, revising the time frame to three years seems inconsistent with this constantly changing vulnerability environment. Consider modifying the time frame to annually, or less.
No
No
This CIP does not address how third parties (consultants, contractors, vendors, etc.) should handle BES Cyber System information. Where 3rd parties have persistent or ephemeral remote access to Cyber Assets, they have implicit access to BES Cyber Asset information. NERC could consider applying all information requirements of CIP 011 to any 3rd parties with such access.
Group
Dominion
Connie Lowe
Yes
No
Yes
CIP-008-5-R2 - Part 2.1 Remove the acronym "BES" to be consistent with all the other requirements. Include in measures as an example, "dated evidence of a lessons-learned report from an actual cyber security incident".
No
Yes
Yes
CIP-009 R1: - Part 1.1: change the measures to be "Evidence may include, but is not limited to, one or more plans that include language identifying general conditions for activation of the recovery plan(s)." - Part 1.4 is confusing as written and should be rephrased with "Validate the successful completion of backup processes for information essential to BES Cyber System recovery directly associated with a significant production change" - Part 1.5 should be reworded as " Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of any Cyber Security Incident that triggers activation of the recovery plan(s).". By replacing the word "event" with Cyber Security Incident adds clarity to which events require data preservation. CIP-009 R2: - Part 2.3 should be reworded to be "Test a representation of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." Rationale: All high impact BES Cyber Systems are already subject to other NERC Standards that require testing of backup and recovery of

components on a yearly basis. CIP-009 Application Guidelines - For consistency, CIP-009 should have a published Application Guidelines. No Application Guidelines exist for this Standard.

No

Yes

No

CIP-010-1-R1 - The term "BES Cyber Asset" should be replaced with "applicable Cyber Asset" to better align with the Applicability column - Part 1.1.5 should be clarified to identify only those patches applied to the asset at the time the baseline is established and not all possible historic patches available for the asset. The language of the requirement should be, " Any security patches applied to the applicable Cyber Asset." - The measures of 1.1 need to be updated to be consistent with the "or by group" language of the Requirements such that both bullet points add "or group" after the term "Cyber Assets". The proposed language for the measures would read, " Examples of acceptable evidence include:..." • A spreadsheet identifying the required items of the baseline configuration for each Cyber Asset or group; or • A record in an asset management system that identifies the required items of the baseline configuration for each Cyber Asset or group." - Part 1.3 needs to define specifically the expected documentation requirements from CIP-005 and CIP-007 for clarity. Additionally, the Applicability columns of CIP-005 and CIP-007 for the associated documentation requirements should match the appliability column of Part 1.3. - Similar to Part 1.3, Part 1.4.1 needs to define specifically the expected documentation requirements from CIP-005, CIP-006, and CIP-007 for clarity. - The language in Part 1.4.1 which essentially allows an impact analysis to be performed to determine which controls may need to be retested after the change should be retained. - Part 1.4.2: "BES Cyber Asset" should be replaced with "applicable Cyber Asset" as noted previously - Part 1.5.1 should be altered to, "Prior to implementing any change in the production environment, test the changes in a test environment that models the baseline configuration or in a production environment where the test is performed in a manner that minimizes adverse effects to ensure that required cyber security controls are not adversely affected; and". The parenthetical expression adds no value. - Part 3.1 needs to define specifically the expected documentation requirements from CIP-005, CIP-006, and CIP-007 for clarity. - Part 3.2 replace the language of the requirement with the following: "Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the production baseline configuration of the Cyber System or in a production environment where the test is performed in a manner that minimizes adverse effects. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in baseline configuration between the test and production environments." The parenthetical expression adds no value - Part 3.3 should be reworded for clarity as follows: " Prior to adding a new Cyber Asset perform an active vulnerability assessment of the new Cyber Asset except 1) for CIP Exceptional Circumstances and 2) performing like replacements of the same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset." - The language of Part 3.4 should be changed to, "Document the results of the assessments and the action plan to remediate or mitigate vulnerabilities identified, if any, in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items." The term "if any" was added to denote the need to document the results of assessments that identified no vulnerabilities.

No

No

CIP-011-1 - Part 1.1 clarify intent by rewording with the following suggested language "One or more documented and implemented methods to identify information or information repositories as meeting the definition of BES Cyber System Information." - Part 2.1 needs to be simplified as: "Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information , the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset." The second paragragh adds no additional value and the term "chain of custody" implies a legal definition that goes beyond what we understand is the intent of the requirement. Also, the second bullet should be eliminated in the Measures section for consistency. The following bullet should be removed, " If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, a chain of custody record that was maintained." - Part 2.2 needs to be simplified as " Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, 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 second paragragh adds no additional value and the term "chain of custody" implies a legal definition that goes beyond what we understand is the intent of the requirement. The fourth bullet in the measures section should be removed for consistency with the removal of the second paragraph in the requirements. The following bullet should be removed, " If removed from the Physical Security Perimeter prior to action taken to prevent unauthorized retrieval of information, chain of custody record that was maintained."
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
Yes
Yes
No
Yes
Yes
Please remove R1 Part 1.5 since this Requirement is not related to asset recovery. Most companies already include event analysis of system failures as an engineering practice. This could be included in Guidance as a suggestion. If the intention is to provide data for forensics, then this should be included in cyber security incident response planning (CIP-008) not CIP-009.
No
Yes
Yes
(Comment 1) We agree that documentation should be part of the change process. We agree with the SDT's approach of using CIP-010-1 R1.3 to require updating of documentation when a baseline configuration changes. We prefer this to the current CIP version 3 requirements (CIP-005-3 R5 and CIP-007-3 R9) to review and update documentation. (Comment 2) R1.4.1 references to "cyber security controls identified in CIP-005, CIP-006, and CIP-007" are too vague and open-ended and subject to auditor interpretation. This could be interpreted as requiring a full vulnerability assessment on devices within the ESP after a change to a single system. We suggest limiting the determination and verification of potential affected controls to the specific BES Cyber System that is being changed. Also, we suggest providing information in the guidance section on controls to be considered similar to the guidance that was provided for CIP-010 R3.
Yes
Yes
For clarity, we recommend deleting the second paragraph in each of requirement 2.1 and 2.2 and creating a third sub-requirement (2.3) that states "If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain chain of custody, which identifies who has possession of the device while it is outside of a Physical Security Perimeter."
Individual
Chris Plensdorf
Detroit Edison Company
Yes
Yes
Yes
Yes
Yes

Yes
No
No
Yes
We are concerned that the SDT does not understand the extent of work necessary to meet proposed requirement CIP-010 R1.1.5. Based on requirement 1.5, the baseline required for each cyber asset may change frequently and require documentation of a new baseline monthly as the asset is patched for security vulnerabilities. The term baseline may be inappropriate for this requirement as it us written. Perhaps the term configuration log would be more appropriate. We found the language in requirement CIP-010 R2.1 to be amiguous and confusing as it may suggest that twice per 35 calendar days is non-compliant which would certainly then mean that continuous is non-compliant also. Possibly replace "not to exceed once every 35 calendar days" with "not less than once per 35 calendar days"
Yes
Yes
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
Yes
(1) Regarding CIP-008-5, R1.1 and R1.2 need to allow for one or multiple processes. Southern suggests changing to ‘one or more processes’ throughout the standard. (2) Regarding CIP-008-5, R1.1 and R1.4 are essentially redundant. ‘Respond’ in R1.1 and ‘handling’ in R1.4 are the same. Southern suggests deleting R1.4 to avoid unnecessary duplication. (3) Regarding CIP-008-5, R1.5, Southern suggests changing “that should receive communication” with “that must be sent communication”. Southern also suggests changing the “individuals and” to “individuals or” to help eliminate double jeopardy issues with EOP-004 which specifies the external communications. (4) Regarding CIP-008-5, R2.1, Southern suggests changing “BES Cyber Security Incident response plan(s)” to “incident response plans identified in R1”. R2.2 follows this approach and it avoids the awkward combination of a definition in the name of a plan. (5) Regarding CIP-008-5, R2.1 needs clarification that if an entity has numerous response plans if[?]each one must be tested every year. (6) Regarding CIP-008-5, R2.1 Measures include a specific lessons learned dated report which is not part of the requirement. Southern suggests deleting “a lessons-learned report” from the Measures. (7) Regarding CIP-008-5, R2.2 reads as though only one test plan can exist which is in conflict with R2.1. Southern suggests that the language be changed to allow for multiple plans to exist. (8) Regarding CIP-008-5, R2.3, is there double jeopardy here with record retention requirements in EOP-004? Southern suggests removing R2.3 and let EOP-004 handle all aspects of reporting and retention. (9) Regarding CIP-008-5, R3.4, Southern suggests returning to V4 language. It seems that to audit this requirement a master list of “technology changes” would need to be produced with an analysis of which ones did or did not affect any incident response plans. A date for each “technology change” would also be required in this master list so the 30 day clock can be audited.
No
No
Yes
(1) Regarding CIP-009-5, R1.3, Southern suggests striking the word “successfully” in the measure. (2) Regarding CIP-009-5, R1.4 needs to have provisions for vendor or other 3rd party backups or the initial media. If what is needed to recover a system is simply a reload from the vendor software CD, how does an entity prove that it was verified initially? Southern suggests adding to the beginning of the requirement “Responsible Entity created backups of information essential…”. Additionally,

Southern strongly suggests that the requirement be reworded to match the Measure. Proposed language, “The backup process for information essential to BES Cyber System recovery that is stored on backup media shall be verified to ensure the backup process completed successfully.” (3) Regarding CIP-009-5, R1.5 needs additional conditions for invocation [?]. Some activities captured within the requirement are normal course of business vs. cyber attack. A malfunctioning motherboard after a known power surge or lighting strike should not invoke a forensics process. Southern suggest replacing “any event” with “Reportable Cyber Security Incident” to address when forensics is required. (4) Regarding CIP-009-5, R2.1, an entity could have hundreds of recovery plans for all different types of systems. Is it permissible to test one plan for each representative type of cyber system or must it be shown for every individual BES Cyber System as per the applicability column? If so, this should be clarified in the requirement. Additionally, consider if “or” is needed after the first bullet, as shown in the second bullet. (5) Regarding CIP-009-5, R2.2 could imply that if daily backups are taken, every one of those daily backups should be tested annually. The requirement should not require the test of a year’s worth of backup tapes, just the last one or a representative sample. It takes too long of a period of time to restore every backup and would be a waste of resources. Proposed text: “Test a representative sample of information used in the recovery of BES Cyber Systems that is stored on backup media, at least once each calendar year, not to exceed 15 calendar months between sample tests, to ensure that the information is useable and is compatible with current system configurations.” (6) Regarding CIP-009-5, R2.3 needs additional clarity that all recovery plans do not have to be “fully operationally tested” at the same time. Utilities need the flexibility to test individual recovery plans at different times within the three-year period. Southern proposes replacing the second occurrence of “plans” with “plan” in the first sentence of the requirement. Additionally, the initial test for this particular requirement needs to be within the first full 3-year period following the compliance date. (7) Regarding CIP-009-5, R3.4, the focus of the requirement should be on “notification” not “distributing”. Proposed text: “Notify responsible individuals under R1.2 of recovery plan updates within 30 calendar days of the update being completed.”
No
No
No
(1) In general regarding draft 2 of CIP-010-1, Southern strongly suggests that the SDT return to the approved language in CIP-003-4 R6 and CIP-007-R1 with targeted and efficient changes to address FERC orders. (2) Regarding CIP-010-1 R1, R1.1.1 Southern suggests changing “exists” to “is either operating or running”. (3) Regarding CIP-010-1 R1, R1.1.5 changes too frequently to be in the baseline and should be removed. The evaluation of each patch is already included in CIP-007-5. (4) Regarding CIP-010-1 R1, there is opportunity for double jeopardy with R1.1.4 and R1.1.5 and CIP-007 that could be resolved by making CIP-010-1 activities distinct from CIP-007-5 required activities. (5) Regarding CIP-010-1 R1, R1.3 creates opportunity for double jeopardy and needs to be revised or removed. (6) Regarding CIP-010-1 R1, R1.4.1 should be deleted and the word “applicable” added into R1.4.2. This would eliminate the extra documentation step represented by R1.4.1. Southern believes R1.4.1 where “could be impacted” is used will cause all entities to document every control for every change in order to avoid zero-defect audit enforcement when some situation can be devised where “could be impacted” is a remote possibility. Southern believes that documenting “what could be impacted” is not a reliability benefit, it’s the verification that controls are not affected by a change. (7) Regarding CIP-010-1 R1, R1.4.2 we suggest deleting “and the BES Cyber System availability”. If a change such as a vendor patch causes an unforeseen outage on a single device, is that a cyber security violation? (8) Regarding CIP-010-1 R1, as written, it’s not clear what the essential difference is between R1.4 and R1.5 is for High Impact Systems. Additionally, there appears an opportunity for double jeopardy in R1.4 and R1.5. Southern recommends removing the overlap in applicability of the two requirements and adding clarifying language as to what is intended and required in R1.4 vs. R1.5. Simpler, higher-level language needs to be developed for R1.4 and R1.5. Both are confusing as to what is expected and how they do or don’t relate to one another. (9) Regarding CIP-010-1 R3, proposed text for R3.1: “At least once every calendar year or not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment (leveraging previous cyber security controls test results where possible) to determine the extent to which identified cyber security controls are implemented correctly and operating as designed.” Rationale for Changes to R3.1: For reasons stated earlier in comments and in agreement with EEI’s comments, the “At least once every calendar year, not to exceed 15 calendar months” needs to be replaced with “At least

once every calendar year or not to exceed 15 calendar months." Additionally, it is not apparent what "cyber security controls" exist in CIP-006. CIP-006 defines physical security controls and should not be listed in this requirement as it is duplicative of the testing and maintenance already required under CIP-006-5. Additionally, this requirement, by referring to other standards, creates a double jeopardy situation. The dependency on other standards needs to be removed and replaced by "identified cyber security controls". Additionally, for efficiency, the requirement needs to leverage the cyber security control reviews that are already being conducted in other standards, and require an additional new assessment only if one has not been already conducted in the previous 15 months. This clarification needs to be explicit in the requirement and added to guidance. (10) Regarding R3.2, it's not clear how this requirement is different from what is already required in CIP-007. (11) Regarding R3.4, replace "remediate or mitigate vulnerabilities" with "implement lessons learned (if any)" for consistency with other standards and eliminate extra documentation tracking requirements. Proposed text: "Document the results of the assessment and the action plan to implement lessons learned (if any) identified in the asessments including the proposed date of completing the action plans."
Yes
No
(1) Regarding CIP-011-5, R1.1 and R1.2, Southern suggests deleting the phrase "and implemented" as it is a duplicate of the verb in the main Requirement. (2) Regarding CIP-011-5, replace "to remediate deficiencies" with "for lessons learned (if any)". This is a find and fix requirement and should not be a compliance violation. (3) Regarding CIP-011-5, the term "chain of custody" has a well understood legal definition not appropriate for the NERC CIP standards. The focus of 2.1 and 2.2 needs to return to the CIP-003-4 R4 and R5 language. Replace "maintain of chain of custody" with "maintain a process to document the control of the device". Additionally, the term "chain of custody" needs to be removed from the measures. (4) Additionally regarding CIP-011-5, R2.1, the requirement of "who has possession" needs to be removed as the process to document control of the device may include couriers or external vendors.
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
R1.1 - Replace "Processes" with "Process(es)". You could have just one process. R1.5 - Replace "that should" with "must", and "receive communication" with "be sent communication". Replace "individuals and" with "individuals or". This limits double jeopardy related to external organization communications which are included in EOP-004 requirements. R2.3 - EOP-004 record retention requirements may result in double jeopardy, this requirement is redundant and should be removed.
Yes
Yes
Yes
R1.3 - In measures remove "successfully". R1.4 introduces questions about response for when a backup fails. If a single monthly backup succeeds, is that good enough? What is verified initially? Is this a daily check for backups or is weekly verification sufficient? If a log is printed or a snapshot taken monthly for evidence sufficient if alerting to x-number of failures is part of the process or is evidence collection required upon completion of the backup? R1.5 - Need to have provisions to identify that this is as a result of a malicious threat and not process or equipment fault.
Yes
Yes
Yes
R1 requires additional personnel and systems to accommodate the expansion of test and acceptance environments to meet new test requirements. R1.1 - 1.1.4 and 1.1.5 are duplicates of CIP 007 and CIP 010. Would create double jeopardy consolidate in one place. R1.4 - consider dropping 1.4.1, this is covered in 1.4.2. Move CIP-005, CIP-006, and CIP-007 statement into 1.4.2. Strike "and the BES

Cyber System availability” from 1.4.2. R3.4 - Replace “remediate vulnerabilities identified with “incorporate lessons learned”.
Yes
Yes
R1.3 - Replace “remediate deficiencies identified" with “incorporate lessons learned”.
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form C.
Individual
Ralph Meyer
The Empire District Electric Company
No
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term “…but not limited to…” 3. Change all instances of Medium Impact BES Cyber Systems to “Medium Impact BES Cyber Systems with External Routable Connectivity” for consistency with CIP-005, CIP-006, and CIP-007 4. CIP-008 R1.2 requires the Plan to have: A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident. The definition of Reportable Cyber Security Incident is in the definitions as “Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.” As written the Entity is to develop a process to determine if a cyber security incident compromises or disrupts a reliability task. But the list of reliability tasks is not defined in the Standards. Suggested changes to definition of Reportable Cyber Security Incident, to also be included in the requirement a. Suggestion 1) Any Cyber Security Incident that has disrupted the operation of the BES resulting in a violation of a SOL or IROL. b. Suggestion 2) Any Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. 5. R2 – Allow for an exception to the time frames listed in the event of CIP Exceptional Circumstances 6. R2.1 a. Remove the word “BES” from the Requirement to be consistent with R1. b. Remove the words “lessons-learned report that includes a” from the Measures because the following items do not necessarily fall into the lessons learned category. c. Add a 2nd Measure “OR documentation from an actual Reportable Cyber Security Incident” as an alternative to the listed evidence. 7. R3.1: Change the Requirement to read “Review and update each Cyber Security Incident response plan for accuracy and completeness once each calendar year or a period not to exceed 15 calendar months between reviews except for CIP Exceptional Circumstances.” Rationale: Reduce significant confusion 8. R3.2 a. Clarify Requirement as follows: “R.3.2 “Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” b. Clarify Measures as follows: “Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident

Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change." 9. R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
No
No
No
10. R3: In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates." R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and
No
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term "…but not limited to…" 3. R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. 4. R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 5. R2: remove Associated assets/systems from applicability because they go beyond Order 706. 6. R1.1: Add "with External Routability" to Medium Impact BES Cyber Systems 7. R1.4: Remove "High Impact" from Applicability because it is repetitious with R1.5. 8. R3.1 a. Applicability: Add "with External Routability" to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets. b. Requirement: Change to read: "At least once every calendar year, or up to 15 months between assessments, conduct a paper and/or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed. Any paper and/or active vulnerability assessment already performed in the implementation of other CIP standards are not included in this requirement". Rationale: avoid double jeopardy. 9. R3.2: Remove the words "that models the baseline configuration of the BES Cyber System in a production environment" after the parentheses. 10. R3.3: Change the words "prior to adding" to "as part of the

change prior to completing the commissioning of". Rationale: clarity 11. R3.4: Change the requirement to read: "Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities." Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
No
No
1. In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. 2. In all measures section remove the term "…but not limited to…" 3. Applicability for all requirements should add "Medium Impact BES Cyber Systems with External Routability" to all "Medium Impact BES Cyber Systems" 4. Several requirements use the terminology "BES Cyber System Information", however this creates an inconsistency with all the "Associated…" assets in the Applicability column. Suggestion is to leave the applicability in that column, and don't name asset/system types in the requirement. 5. The length of the "Applicability…" column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to "Applicability". 6. R2 uses the term "chain of custody" in several places. This is a legal term that relates to evidence. Suggest replacing it with "possession" or "control". 7. R1.3: Change Requirement & Measure language time frames by removing "at least" and replacing with "once each calendar year or a period not to exceed 15 months". 8. R2.1: In parenthetical text in Requirement change to read "(except for reuse in other high impact…)" for clarity.
Individual
Kirit Shah
Ameren
Yes
Yes
Yes
(1) General Comment – For all the measures for CIP-008 the wording "with External Routable or Dial-up connectivity" should be added to the applicability of Medium Impact BES Cyber Systems due to the added amount of documentation that would be needed for no additional security benefit to the BES. (2) R2.1 – Remove the words "BES" in front of the words "Cyber Security Incident" from the requirement to match the references to "Cyber Security Incident" in all the other requirements for CIP-008. (3) R2.1 - Insert "or" after the first bullet in the requirements. As currently worded entities must perform 2 of the 3 exercises to meet compliance. (4) R2.3 – Remove 'relevant' in the requirements or clearly define what relevant records are to eliminate subjective interpretation (perhaps refer to M2.3 within the requirement).
Yes
Yes
Yes
(1) R1.3 – The words "and associated system" needs to be added after "BES Cyber System" in the requirements and measures to clarify that this requirement applies to the associated systems. (2) R1.4 – (a) The requirement should be reworded to "Information essential to BES Cyber System recovery that is stored on backup media shall be verified after each backup to ensure that the backup process completed successfully." (b) The words "for 90 days" need to be added after the word "logs" in the measures. Currently there is no time frame for how long these logs need to be retained. (3) R2.1 - Insert "or" after the first bullet in the requirements. As currently worded entities must perform 2 of the 3 exercises to meet compliance. (4) R2.3 – The requirements asks entities to perform a functional test of the recovery plans every 36 calendar months. What M&T or DR industry standard does the 36 month recommendation come from? We suggest that some guidance be added to the standard to explain why 36 calendar months was selected.
No

Yes
Yes
(1) General Comment – (a) For all the measures for CIP-010 the wording "with External Routable or Dial-up connectivity" should be added the applicability of Medium Impact BES Cyber Systems. Currently technology does not exist to meet compliance with these requirements for serial connected devices; for example programmable protective relays. (b) For all the applicability for CIP-010 remove "Associated Protected Cyber Assets" to match the current CIP standards. (2) R1.1 – We request that the requirement be reworded to "Develop a baseline configuration for each Cyber Asset identified, individually or by group. The requirements in 1.1.1 to 1.1.5 go above and beyond what most baseline software can do today and would require manual inventorying of baseline systems instead of using automated process. (3) R1.4 – Remove "High Impact BES Cyber Systems" from the applicability since High Impact BES Cyber Systems is covered in R1.5. This requirement is confusing since this requirement is also covered in R1.5 (4) R2.1 – We request a change of wording for “monitor continuously or periodically, not to exceed once every 35 calendar days” to “document changes tracked through the Entity’s change management program” in the requirement. To check the baseline configuration of every system will be overly burdensome to entities. We suggest changing the 35 calendar day requirement to every 90 days.
Yes
No
(1) General Comment – For all the measures for CIP-011 the wording "with External Routable or Dial-up connectivity" should be added the applicability of Medium Impact BES Cyber Systems. Currently technology does not exist to meet compliance with these requirements for serial connected devices; for example programmable protective relays. (2) R2.1 – The Applicable section needs to be adjusted or requirement changed to reflect BES Cyber Systems and Associated systems that do not need to be in a Physical Security Perimeter. We would suggest removing the words "Physical Security Perimeter" and replace with "secured area" to help clarify this requirement. (3) R2.1-R2.2 – The SDT had stated “Chain of Custody” for all devices while outside of the ESP in the requirements. Please clarify what is the intent of “Chain of Custody.” Is it the intent of the SDT to require hermetically sealed evidence containers that are not accessed through the same opening more than once and every person accessing the device has a personally identifiable seal? We suggest using different wordings or an approach such as retired asset must remain in the custody of the entity at all the time.
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
CIP-011 R2: SRP suggests adding further detail on what qualifies as protected information. This would assist entities in identifying said information. Current verbiage allows for entity interpretation.
Group
Associated Electric Cooperative, Inc. (NCR01177, JRO00088)

David Dockery, NERC Reliability Compliance Coordinator, AECI
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
No
No
No
(1) The applicability of CIP-008-5 R1, R2 and R3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would support the current applicability and proposed changes to the applicability of CIP-005-5, CIP-006-5 and CIP-007-5 and would align the incident response plan to those cyber systems that have connectivity. (2) CIP-008-5 R2.3 requires retention of relevant records and should be relocated to Section C1.2 regarding Evidence Retention. (3) Combine Requirement R3.2 and R3.3 and allow 60 calendar days to complete the investigation, determine appropriate lessons learned, and update the response plan. (4) The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents.
No
Yes
No
(1) Combine Requirement R3.2 and R3.3 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s). (2) In Requirement R3.3, 30 days should be extended to 60 calendar days to make the overall timing for the activities in R3 more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan.
(1) The applicability of CIP-009-5 R1.1, R1.2, R1.3 and R1.5 should be limited to “Medium Impact BES Cyber Systems at Control Centers.” This will concentrate efforts on areas where reliability impacts are the highest and avoid placing additional/duplicate requirements on cyber systems/assets covered under the PRC Standards. (2) The misoperation of relaying systems is covered under the PRC Standards and should be excluded from CIP-009-5 R1.5. (3) Comments on CIP-009-5 R3 are in Question 7 Comments.
No
Yes
No

(1) The applicability of CIP-010-1 R1.1, R1.2, R1.3 and R1.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” Consider limiting to Control Centers only. As the requirements are currently written, they mandate the creation of an asset register for a large population of cyber assets that are not connected to a network via a routable protocol and are already covered under the PRC Standards. This will place an undue burden on the Responsible Entity without enhancing reliability. (2) Split Requirement R1.3 into two Requirements. For High Impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, leave the requirement at 30 days. For Medium Impact BES Cyber Systems with External Routable Connectivity, Associated Electronic Access Control or Monitoring Systems, and Associated Protected Cyber Assets, extend time to 60 days to allow for sufficient time to process/document the required changes and verifications. (3) The applicability of CIP-010-1 R3.1 and R3.4 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports the proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity.
No
No
The applicability of Requirements R1.1, R1.2, R1.3, R2.1, and R2.2 should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
R3, Part 3.4 requires an update to an entity’s Cyber Security Incident response plan(s) within 30 calendar days of certain changes (plan roles/responsibilities or technical). The preceding R3 requirements require plan updates (as needed) based on lessons learned through application of the plan through a test or actual incident and at a minimum the plan must be reviewed and updated annually. FE believes that R3, part 3.4 will subject responsible entities to undue compliance burden that is best left as a best practice and not a mandatory and enforceable reliability requirement. The reviews and updates occurring through the lessons learned (3.2, 3.3) and the annual plan reviews (3.1) should suffice for the updates needed.
Yes
Yes
Yes
R3, Part 3.3 requires an update to an entity’s recovery plan(s) within 30 calendar days of certain changes (plan roles/responsibilities or technical). The preceding R3 requirements require plan updates (as needed) based on lessons learned through application of the plan through a test or actual incident and at minimum the plan must be reviewed and updated annually. FE believes that R3, part 3.3 will subject responsible entities to undue compliance burden that is best left as a best practice and not a mandatory and enforceable reliability requirement. The reviews and updates occurring through the lessons learned should suffice for the updates needed.
No
Yes
Yes
R1 refers to baselines and what is desired via the requirements appears to be documentation of the current configuration of the Cyber Asset. The main goal of FE’s proposed change (see following text)

is to eliminate the word "baseline". FE believes a risk exists to confuse the purpose with security baselines we create today for devices. The following is draft language proposed for R1. R1.1 Document the configuration, which shall include the following for each Cyber Asset identified, individually or by group: R1.1.1 - R1.1.5 no changes R1.2 Authorize and document changes, individually or by group to each Cyber Asset identified that would affect: R1.2.1 Operating system(s) (including version), or firmware where no independent operating system exists; R1.2.2 Any commercially available or open-source application software (including version) intentionally installed on the BES Cyber Asset; R1.2.3 Any custom software developed for the entity; R1.2.4 Any logical network accessible ports; and R1.2.5 Any security patches. R1.3 For a change identified in R1.2 update configuration documentation for each Cyber Asset identified and other documentation required by CIP-005 and CIP-007 as necessary within 30 calendar days of completing the change. R1.4 For a change identified in R1.2: R1.4.1 - R1.4.3 no changes R1.5 Where technically feasible, for each change identified in R1.2: R1.5.1 - R1.5.2 no changes
Yes
Yes
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
No
Yes
Yes
(R1) It is not clear how the process to respond to Cyber Security Incidents required by R1.1 differs from the procedure to handle Cyber Security Incidents required by R1.4. Whatever distinction there might be is further muddled by the fact that the measure for R1.4 includes both processes and procedures and refers to a response as well as to “handling” the incident. We recommend that R1.4 be deleted or the requirements be rewritten to clarify the distinction between the requirements.
No
No
No
(Part 3.2) R3.2 The measure should address the anticipated evidence for a situation where there are no deficiencies. Do you require documentation within 30 days stating that there were none, or is an attestation at a later date adequate? (Part 3.4) In R3.4 “Distribute” is the wrong word and should be replaced with “make available”. Distribute implies actively sending someone the document. A change will frequently affect only a small subset of the people responsible for the plan. An email summarizing the changes and containing a link to the new version is the typical way of handling this and is completely adequate to support the purpose of the requirement
(Part 1.4) R1.4 does not fit with the parent requirement or with the other subrequirements. R 1 is about what the plan must contain. R1.4 is for a specific action (verifying backup data). You could state that the plan must have a process for verifying backup data or you could move this to a separate requirement, but it does not belong here as written. (Part 1.5) R1.5 is too vague. Specifically, it does not provide entities with adequate information to determine what data needs to be preserved. This requirement could reduce reliability. The measure implies a requirement to mirror data before proceeding to recovery. First it is improper to include a requirement in a measure; second, it should be left to the entity whether understanding the cause of the failure is important enough to justify delaying recovery to preserve this data (whatever it is eventually specified to be). Thirdly, there are a multitude of ways a system can fail, and it is not reasonable to develop processes for each possibility. Although we agree that a fault analysis is a worthy endeavor, we do not believe it is measureable enough to be written into the standards at this time. We believe the R3.1 requirement to conduct a post incident analysis is sufficient to address the continual improvement of processes and technology. Finally, the last part of the measure, a procedure for "taking the important assessment steps necessary to avoid reintroducing the precipitating or corrupted data" does not seem to provide evidence of "processes to preserve data . . . for analysis or diagnosis" (Part 2.2) The measure for R2.2 requires evidence of a test when it is initially stored; the requirement no longer includes this. The measure should be modified to match the current draft of the requirement. It is not

clear whether an entity must test all information or a sample of the information to comply with this requirement. Please clarify. (Part 2.3) A recovery plan may be comprised of one overall plan with a number of underlying processes for different failure scenarios, each of which may have different variations based on the details of the failure. It is not clear whether an entity needs to test, 1) the overall plan using at least one of the underlying processes, 2) the overall plan and each underlying process, or 3) every possible variation of the plan and processes.
Yes
Yes
Yes
(Part 1.1) Why is "BES Cyber Asset" used in 1.1.2 and only Cyber Asset used in 1.1? In R1.1.3 Consider deleting “developed for the entity”. It appears that the intent is to capture all software in 1.1. As written the requirement could exclude custom software such as scripts that were originally developed for another entity. (Part 1.3) In R1.3 Greater specificity is needed regarding the documentation required under CIP -005 and CIP-007 that must be updated. We don’t believe that this requirement captures what the SDT intended. R1.5 requires updates only when the baseline is altered. For example, a network could be reconfigured significantly without any change in the baseline, but with substantial changes in network diagrams etc. R1.3 would not require an update in that case. Consider requiring an update of relevant documentation within CIP005 and CIP-007 in those standards instead of in CIP 010. (Part 1.5) R1.5.2 Consider deleting the portion of the requirement from the word “including” on. It may not be worthwhile to take measures to account for differences between the test and production requirements. Additionally, the requirement gives entities no standard about how significant the measures must be. Must they totally account for the differences (this is not achievable without completely replicating your production environment which could be prohibitively expensive). Would a single trivial measure that accomplishes little be sufficient? The requirement states that an entity must describe the measures used but does not explicitly require it to use measures (to account for differences between test and production). Would a statement that no measures were taken be adequate for compliance? Entities need a clear statement of what is expected. If the text is retained, consider allowing as an alternative a statement that the entity is aware of, and accepts the risk of, differences in the environments. (Part 3.1) R3.1 Consider deleting the reference to CIP-006 in this requirement. Entities are already required to test their systems by CIP-006 R3.1. If that test does not adequately cover the scope required we recommend you make the change there instead of having pieces of physical security testing in two separate standards. (Part 3.2) Is the scope of this VA CIP-005 and CIP-007 or did you intend to include CIP-006? We recommend excluding CIP-006 since testing of physical security systems is covered in that standard, but either way, it should be explicitly stated. (Part 3.3) R3.3 To improve clarity consider adding “to determine the extent to which the cyber security controls identified in CIP-005, and CIP-007 are implemented correctly and operating as designed.” We assume you did not intend to require a review of CIP006 at this point, but since it is not describing the scope the requirement specified, it implies that it would be the same as 3.1.
No
Yes
(Part 1.1) In R1.1 and 1.2 the addition of the words “and implemented” is redundant and confusing. The parent requirement already requires the implementation of the program. The additional bullet in the measures is also puzzling. We do not see how “Repository or designated electronic and physical location” would be evidence that an entity has established methods to identify BES Cyber System Information. (Part 1.2) R1.2. Consider changing “or” to “and” in the measures. It seems that you would want both evidence that the procedures had been established and that it was followed. (Part 1.2 and 1.3) R1.2-R1.3 It should be clarified whether a single identified instance of deviation from the Information Protection Program (either identified in the 1.3 assessment or otherwise) would be considered a violation of R1.2. If it is, then the requirement to have an action plan to remediate deficiencies would be duplicative of the entity’s mitigation plan. (Part 2.1 and 2.2) "device" should be replaced with "Cyber Asset."
Individual
Michael Lombardi
Northeast Utilities
Yes

Yes
Yes
Table R1 through R3, Applicable BES Cyber Systems and associated Cyber Assets - Recommend expanding the applicability from “High Impact BES Cyber Systems” and “Medium Impact BES Cyber Systems” to include “Associated Physical Access Control Systems,” “Associated Electronic Access Control or Monitoring Systems” and “Associated Protected Cyber Assets.”
Yes
Yes
Yes
None
None
Yes
Yes
Yes
None
Yes
Yes
Table R1, Part 1.2 - Please clarify: (1) what is meant by transit plus include exclusionary clause as to what it does not mean; (2) what records are required for handling information.
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R3.1 and R3.2 be revised to read as follows (and delete R3.3 and R3.4 to be combined in a new R3.2): R.2.1 “Test the BES Cyber Security Incident response plan(s) at a timeframe deemed necessary by the Responsible Entity: • By responding to an actual Reportable Cyber Security Incident; • With a paper drill or tabletop exercise; or • With a full operational exercise.” R.3.1 “Review and update each Cyber Security Incident response plan for accuracy and completeness at a timeframe deemed necessary by the Responsible Entity.” R.3.2 “Maintain a current and up-to-date Cyber Security Incident Response Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals or (4) technology changes.”
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R2.2, R2.3 and R3.1 be revised to read as follows (and delete R3.2 and R3.3 that will be combined into a new R3.1) R2.1 “Test the recovery plan(s) referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise.” R2.2 “Test information used in the recovery of BES Cyber Systems that is stored on backup media at a timeframe deemed necessary by the Responsible Entity to ensure that the information is useable and is compatible with current system configurations.” R2.3 “Test each of the recovery plans referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity through an operational exercise of the

recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." R.3.1 "Maintain a current and up-to-date Recovery Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals and (4) technology changes."
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R2.1, R2.2, R2.3 and R3.1 be revised to read as follows (and delete R3.2 and R3.3 that will be combined into a new R3.1) R2.1 "Test the recovery plan(s) referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity: • By recovering from an actual incident; • With a paper drill or tabletop exercise; or • With an operational exercise." R2.2 "Test information used in the recovery of BES Cyber Systems that is stored on backup media at a timeframe deemed necessary by the Responsible Entity to ensure that the information is useable and is compatible with current system configurations." R2.3 "Test each of the recovery plans referenced in Requirement R1 at a timeframe deemed necessary by the Responsible Entity through an operational exercise of the recovery plans in an environment representative of the production environment. An actual recovery response may substitute for an operational exercise." R.3.1 "Maintain a current and up-to-date Recovery Plan, including (1) the documentation of any lessons learned associated with a Cyber Security Incident test or actual incident response; (2) roles or responsibilities; (3) cyber Security Incident response groups or individuals and (4) technology changes."
No
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R3.1 be revised to read as follows: "At a timeframe deemed necessary by the Responsible Entity, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed."
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to that suggested by EEI, NextEra believes a Responsible Entity should implement a robust, current and updated CIP compliance program without imposed arbitrary deadlines and a micromanagement of the program. To implement these changes, NextEra requests that R1.3 be revised to read as follows: "At a timeframe deemed necessary by the Responsible Entity, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment."
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
No
No
1- QUESTION 2: We believe there is a typo in bullet 2.2, the "of" in the first sentence should be an "or". Bullet 2.3 is a data retention requirement that is a compliance element, not a requirement (especially in light of paragraph 81 of the FERC Order approving FFTR), and should be deleted. 2- QUESTION 3: Bullets 3.3 and 3.4 cover change management of the Cyber Security Incident response plan and Bullet 3.1 is duplicative and should be deleted (especially in light of paragraph 81 of the FERC Order approving FFTR). Alternatively, bullets 3.3 and 3.4 can be deleted in favor of bullet 3.1. Bullet 3.2 belongs in R2, not R3.

No
Yes
Yes
1- QUESTION 5: Bullet 1.4 uses an ambiguous term “verify”. Does “verify” mean that the information is retrievable from the back-up media, or does it mean that it is identical to the original information? If the latter, then R2 bullet 2.2 is not needed.
Yes
Yes
Yes
Yes
Yes
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
R1.3 – NRECA requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. NRECA believes these deficiencies should not be considered violations and requests that the SDT make this clear in the requirement language.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Yuling Holden
PSEG
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
R3 - the VSL does not address the 36 month timeline in Requirement 3.2 and only the timelines in R3.1. We suggest adding a modification via an "or" statement in all VSLs • Low- An active vulnerability assessment of High Impact BES Systems was completed more than 36 months but less than 39 months since the last one • Medium- An active vulnerability assessment of High Impact BES Systems was completed more than 39 months but less than 42 months since the last one • High- An active vulnerability assessment of High Impact BES Systems was completed more than 42 months but less than 45 months since the last one • Severe- An active vulnerability assessment of High Impact BES Systems was completed more than 45 months since the last one
No
Yes
Measure for R1.2: This measure does not specify what records could be used to indicate consistency with the entity's documented procedures. Please provide guidance as to what acceptable methods could be used for compliance – would sampling work in this case, and if so, what is the acceptable tolerance range for such sampling?
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Yes
Yes
Individual
Daniel Duff
Liberty Electric Power, LLC
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
No
The definition of BES Cyber Information needs to be made clearer regarding assets such as relay test laptops which may leave the control of the RE.
Individual
Don Jones
Texas Reliability Entity
Yes
Yes
No
CIP-008-5 R2 fails include “each” of the applicable items.
No
Yes
Yes
CIP-009-5 R3 does not include defined roles and responsibilities.
No
Yes
No
CIP-010-1 R1 (1.2) does not indicate the appropriate authorizing individual or delegate. CIP-010-1 R3 does not always include Medium Impact in its scope. CIP-010-1 R3 does not define what is comprised by an active vulnerability assessment. CIP-010-1 R3 does not include an annual review, but only enforces a review every 36 calendar months.
No
Yes
CIP-011-1 R1 does not mandate the identification of protected information (e.g. confidential).
Individual
Don Schmit
Nebraska Public Power District
Yes
No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards. I do not believe that they have fully resolved these issues. CIP 8 R2.2 – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. CIP 8 r3.1 – Suggest strike “and update” to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage “update, if necessary.” CIP 8 r3.5 – Suggest striking “distribute”. What constitutes distribution? Suggest retaining “notification” approach.

Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals.
No
No
Yes
Once again it is straightforward to see the objectives the drafters are trying to accomplish, but the reality of this level of descriptiveness and compliance thereof, would be disruptive and prohibitive. CIP 9 r1 – The standard isn't clear whether the recovery plans are for recovery of the asset, system, or function. CIP 9 r1.4 – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes "initial," "verification," or "ensure the process completed successfully"? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: "Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function." CIP 9 r1.5 – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: "Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s)." CIP 9 r2.1 - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a "full operational exercise" on all systems, or is a representative sampling sufficient? CIP 9 r2.2 – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. CIP 9 r2.3 – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a "standby" system for testing. CIP 9 r3.4 – Once again the use of the word "distribution". If I notified a vendor of an update to the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its "distribution".
No
No
No
CIP 10 r1.1.3 – Proposed verbiage: "Any custom compiled software" CIP 10 r1.4 – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. CIP 10 r2.1 – Recommend replacing "technically feasible" with "Within the capabilities of the system or network configuration." Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or quarterly verification, because a manual process of verifying the baseline will be administratively burdensome. CIP 10 r3 – What is the definition of an "active vulnerability assessment"? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an "active vulnerability assessment" on all systems, or is a representative sampling sufficient? Recommend striking "CIP-006" from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months.
Yes
Yes
[R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of

“confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts.
Group
Luminant
Rick Terrill
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
For all Luminant responses and comments, please see the group comments submitted by the Texas RE NERC Standards Review Subcommittee.
Individual
Stephanie Monzon
PJM Interconnection
Yes
No
No
R2 – This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 8 R2 & R3 we picked out records, technology change, and routable. If we knew what NERC’s intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. The words restore & recovery mean different things depending on the area being examined R3 – Please ensure that the verbiage on “any changes” more in line with CIP 9
No
No
No
R2 – This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 9 R1, R2 & R3 we picked out recover, restore, operational exercise, & technology change. If we knew what NERC’s intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. The words restore & recovery mean different things depending on the area being examined R3 The following phrasing is helpful and similar verbiage should be used elsewhere when referencing evidence: Evidence may include, but is not limited to, dated documentation reflecting changes made to the recovery plan(s) in response to the following changes that the responsible entity determined would impact the plan or the ability to execute the plan: • Roles or responsibilities; or • Technology changes.
No

No

No

R1.1 Port should be updated to say ports & services This comment actually applies to all CIP requirements in that an expanded glossary would be extremely helpful. Much of the discussion surrounding the review of requirements is trying to determine NERCs meaning of a word vs our meaning of a word. Here in CIP 10 R1 we picked out Baseline & differences in operation.. If we knew what NERC's intent of what that means we would be better prepared to understand how our measures met the requirement. The meanings of words are also situational from requirement to requirement. Baseline could be implemented many different ways depending on a company's individual strategy R1.5.1 By using the word "model" rather than identical we assume that there is flexibility with the differences between the state and scope of production vs test R2.1 Remove the words continually, it insinuates real time monitoring This can be interpreted as not needing to self report and no remediation necessary R3 Please clarify what is meant by Electronic Access Control or Monitoring Systems R3.3 A cyber asset can be placed into an ESP before remediations of identified vulnerabilities? R3.4 "the planned date of completing the action plan" - is this the completion of the formulation of the plan or the completion of the tasks within the plan?

No

No

R1.2 – "One or more documented and implemented procedures for handling BES Cyber System Information, including storage, transit, and use." Should be for the secure handling of BES Cyber.....

Group

Edison Electric Institute

David Batz

(1.) In all requirements in all standards, and in rationale & guidelines, remove references to systems & assets and rely on the applicability column to specify applicability. Replace globally with Applicable Cyber Systems in rationale and guidance. (2.) In all measures section remove the term 'but not limited to' (3.) Change all instances of Medium Impact BES Cyber Systems to 'Medium Impact BES Cyber Systems with External Routable Connectivity' for consistency with CIP-005, CIP-006, and CIP-007 (4.) CIP-008 R1.2 requires the Plan to have: A process to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident. The definition of Reportable Cyber Security Incident is in the definitions as 'Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity.' As written the Entity is to develop a process to determine if a cyber security incident compromises or disrupts a reliability task. Suggested changes to definition of Reportable Cyber Security Incident, to also be included in the requirement a. Suggestion 1) Any Cyber Security Incident that has disrupted the operation of the BES resulting in a violation of a SOL or IROL. b. Suggestion 2) Any Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. (5.) R2 - Allow for an exception to the time frames listed in the event of CIP Exceptional Circumstances (6.) R2.1 a. Remove the word 'BES' from the Requirement to be consistent with R1. b. Remove the words 'lessons-learned report that includes a' from the Measures because the following items do not necessarily fall into the lessons learned category. c. Add a 2nd Measure 'OR documentation from an actual Reportable Cyber Security Incident' as an alternative to the listed evidence. (7.) R3.1: Change the Requirement to read 'Review and update each Cyber Security Incident response plan for accuracy and completeness once each calendar year or a period not to exceed 15 calendar months between reviews except for CIP Exceptional Circumstances.' Rationale: Reduce significant confusion (8.) R3.2 a. Clarify Requirement as follows: 'R.3.2 'Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.' b. Clarify Measures as follows: 'Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.' (9.)

R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
(1.) In all measures section remove the term 'but not limited to' (2.) In 'Guidelines and Technical Basis' section, list specific FAQs and CIPC guidelines that are applicable. (3.)Remove 'Associated'Systems' from R1-R3 because Order 706 does not require them. (4.) R1.4: a. Replace Requirement language with 'Upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, information essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function.' b. Measures i. What is the evidence retention period' 90 days' Old backup logs are not relevant. ii. What is the evidence of verification' (5.) R1.5 a. In the requirement, replace the word 'event' with 'Cyber Security Incident'. b. In the requirement, add the words 'when it does impact reliability' to the end. (6.) R2.1: Modify the first part of the requirements language to read 'Test a representation of the recovery plans(s) referenced in Requirement R1 once each calendar year or not more than 15 calendar months between tests except for CIP Exceptional Circumstances.' Rationale: Reduce significant confusion. (7.) R2.2 a. Change the first 3 words of the requirement to read 'Test representative information'. b. Measures: Remove the words 'when initially stored and' to be consistent with the requirement. (8.) R2.3: Change the 2nd word 'each' to 'a representation' in the requirement. (9.) R3: In Order 706, paragraph 731, FERC stated 'We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.' We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: 'Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: 'Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates.' R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: 'Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities.'
(1.) In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. (2.) In all measures section remove the term 'but not limited to' (3.) R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. (4.) R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 (5.) R2: remove Associated assets/systems from applicability because they go beyond Order 706. (6.) R1.1-R1.4: Add 'with External Routability' to Medium Impact BES Cyber Systems (7.) R1.4: Remove 'High Impact' from Applicability because it is repetitious with R1.5. (8.) R3.1, R3.4 a. Applicability: Add 'with External Routability' to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets. b. Requirement: Change to read: 'At least once every calendar year, or up to 15 months between

assessments, conduct a paper and/or active vulnerability assessment to determine the extent to which the cyber security controls are implemented correctly and operating as designed. Any paper and/or active vulnerability assessment already performed in the implementation of other CIP standards are not included in this requirement'. Rationale: avoid double jeopardy. (9.) R3.2: Remove the words 'that models the baseline configuration of the BES Cyber System in a production environment' after the parentheses. (10.) R3.3: Change the words 'prior to adding' to 'as part of the change prior to completing the commissioning of'. Rationale: clarity (11.) R3.4: Change the requirement to read: 'Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities.' Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
(1.) In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. (2.) In all measures sections in all standards and requirements remove the term 'but not limited to' The default should be an 'or', and any 'and' should be explicit. Rationale: these are examples only. Using the 'limited to' language creates confusion about whether they're necessary or sufficient. (3.) Applicability for all requirements should be changed from 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routable Connectivity' (4.) Several requirements use the terminology 'BES Cyber System Information', however this creates an inconsistency with all the 'Associated' assets in the Applicability column. Suggestion is to leave the applicability in that column, and don't name asset/system types in the requirement. (5.) The length of the 'Applicability' column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to 'Applicability'. (6.) R2 uses the term 'chain of custody' in several places. This is a legal term that relates to evidence, and is not appropriate in the CIP standards. EEI strongly suggests replacing it with 'possession' or 'control'. (7.) R1.3: Change Requirement & Measure language time frames by removing 'at least' and replacing with 'once each calendar year or a period not to exceed 15 months'. (8.) R2.1: In parenthetical text in Requirement change to read '(except for reuse in other high impact)' for clarity.
Individual
Kathleen Goodman
ISO New England Inc.
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”. For R1.3, and R1.4 wording needs to be added to state that physical security incidents need to be included as well as for Cyber Security Incidents.
No
No
No
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated

Implementation Plan's Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure. Recommend changing from the reference from "R1.2" to "Part 1.2" in R3 Part 3.4 for correctness.
No
No
No
Request clarification of R1 Part 1.1.2. Does "applications" mean "SCADA, EMS, State Estimator, IDC, etc." instead of "device drivers, DLL, applications included in an operating system or package, etc.?" Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software's version? Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part). Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend removing R1 Part 1.4.2 because "availability" has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways. In R1 Part 1.5, recommend changing from "Where technically feasible, for each change that deviates from the existing baseline configuration " to "Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration" for clarity. For R2 Part 2.1, recommend the previous Version 5 words since this updated Part is not understandable. Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations. Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment. Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, "Perform active vulnerability assessment, where technically feasibly….". Recommend that R3 Part 3.3 start with "Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset)." Recommend updating CIP-010 R1's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures shows R1 as "low". Recommend updating CIP-010 R2's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures shows R2 as "low".
Yes
No
The second paragraphs of R2 Parts 2.1 and 2.2 are the same, Recommend removing them from Parts 2.1 and 2.2, and make a new Part 2.3 for clarity.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
No
No
No
CIP-008-5 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-008-5 R1, R2 and R3 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity." This modification would support the current applicability and Oncor's proposed changes to the applicability of CIP-005-5, CIP-006-5 and CIP-007-5 and would align the incident response plan to those cyber systems that have connectivity.

R2 REQUIREMENT COMMENTS: CIP-008-5 R2.3 requires retention of relevant records and should be relocated to Section C1.2 regarding Evidence Retention. R3 REQUIREMENT COMMENTS: The 30-day timing requirement in CIP-008-5 R3.4 should be extended to 60 calendar days such that the overall timing for the activities in CIP-008-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as responses to Cyber Security Incidents. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
Yes
No
R1 APPLICABILITY COMMENTS: (1) Oncor proposes that the applicability of CIP-009-5 R1.1, R1.2, R1.3 and R1.5 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems at Control Centers.” This will concentrate efforts on areas where reliability impacts are the highest and avoid placing additional/duplicate requirements on cyber systems/assets covered under the PRC Standards. (2) The misoperation of relaying systems is covered under the PRC Standards and should be excluded from CIP-009-5 R1.5. R3 REQUIREMENT COMMENTS: The 30-day timing requirement in CIP-009-5 R3.3 should be extended to 60 calendar days such that the overall timing for the activities in CIP-009-5 R3 is more reasonable. This would allow for a consistent 90-day timeline for planned changes as well as lessons learned from the use/testing of the recovery plan. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
No
No
R1 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-010-1 R1.1, R1.2, R1.3 and R1.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems at Control Centers.” As the requirements are currently written, they mandate the creation of an asset register for a large population of cyber assets that are not connected to a network via a routable protocol and are already covered under the PRC Standards. This will place an undue burden on the Responsible Entity without enhancing reliability. R1 REQUIREMENT COMMENTS: Oncor proposes that the 30-day timeline in CIP-010-1 R1.3 should be extended to 90 days (or removed) to allow for sufficient time to process/document the required changes and verifications. R2 REQUIREMENT COMMENTS: Oncor proposes that the 35-day timeline in CIP-010-1 R2.1 should be extended to 90 days to allow for a quarterly review process. R3 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-010-1 R3.1 and R3.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity.” This modification would eliminate existing discrepancies between the applicability of CIP-005, CIP-006, and CIP-007 and the applicability of CIP-010. This modification also supports Oncor’s proposed applicability of CIP-005-5 and CIP-007-5 such that the vulnerability assessments are directed towards cyber systems with connectivity. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
No
No
R1 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-011-1 R1.1, R1.2 and R1.3 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability. R2 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-011-1 R2.1 and R2.2 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity” to maintain consistency with the scope of cyber systems/assets currently covered by similar

requirements in the CIP version 4 Standards. The inclusion of cyber systems/assets with no routable connectivity will significantly increase documentation requirements with no benefit to reliability. GENERAL COMMENTS: (1) Oncor supports the comments submitted by EEI in response to this question. (2) Oncor supports the comments submitted by the Texas RE NERC Standards Review Subcommittee in response to this question.
Group
SMUD & BANC
Joe Tarantino
No
No
No
1. The requirement to document deficiencies or lessons learned Part 3.1 is counter-productive because the requirement will encourage entities to fail to admit that there is a deficiency or lesson in the first place. In the absence of Part 3.1, an entity is more likely to update its plan immediately based upon any newly discovered deficiency. Further, Part 3.1 duplicates the work in the periodic review. In any periodic review, entities will be aware of recoveries made during the period in question and will update their plans accordingly. 2. Enforcement of the provisions 3.1 and 3.2 will be questionable at best, because it is possible that when the plan was exercised, it worked as intended without any identified deficiencies or lessons to be learned. While not stated in the requirements, the entity is left to wonder whether or not it would be in violation if it were not to identify something, and may force the entity to document that the plan worked as intended. This is unnecessarily burdensome to the entity. It is sufficient to have a requirement that the Recovery Plan exists and that it is reviewed for possible changes within prescribed time periods. 3. Exercise of a Recovery Plan does not necessarily lead to the need to update it. Entities will still have the option to update the plan if deficiencies are discovered between the periodic reviews. 4. For 3.1 and 3.2 there really isn't a need for two steps, two separate documents, and time frames for compliance. The same value would be achieved by combining 3.1 and 3.2 into a single item – which is to simply update the test plan within a fixed time frame as a result of deficiencies or lessons learned. Itemized deficiencies or lessons learned could be included in plan document itself. A change log in the Recovery Plan document would accomplish this function. Having two requirements instead of one causes unnecessary exposure to the entity for violations and introduces burdensome administration tasks that are not necessary. Simple is better. 5. Requirement 3.1 states that identified deficiencies or lessons learned from the recovery plan test or incident recovery be documented within 30 calendar days after completion of the test or recovery. Requirement 3.2 requires that the recovery plan be updated based upon any documented deficiencies or lessons learned within 30 calendar days after the documentation required by Part 3.1. This approach has the unintended consequence of encouraging entities to delay the documentation of deficiencies or lessons learned to the end of the 30 day period defined in Part 3.1, because the 30 day period in Part 3.2 to update for the plan begins at the moment the entity documents the Part 3.1 deficiencies. This is a penalty for acting quickly. The approach also makes tracking for compliance overly complicated. To correct this, the periods for both 3.1 and 3.2 should begin as of the date of the completion of the test or recovery. To have similar timeframes without penalizing the entity for acting quickly, the period for 3.1 should begin the day after completion of the test or recovery and be 30 days long. Similarly, the period in which to update the Recovery Plan should begin the day after completion of the test or recovery and be 60 days long.
In Part 1.4, the change to the Measures that change the words "dated evidence of the verification that the backup process completed successfully" to "dated evidence or logs confirming that the backup process completed successfully" is an improvement. It is still not clear, however, that the word "logs" means that employee confirmation that the backup process completed successfully is sufficient. Logs typically imply that there is a requirement for system generated proof. SMUD's original comment is that requiring dated system generated evidence … results in unnecessary administrative burden to the entity because of the never ending need to collect and store evidence repeatedly for many systems. Employee verification that the backup and verification processes were completed via a time-stamped workflow should be sufficient evidence. A: Our comment for this requirement is similar to the prior draft. Changes were made by the team, but our concern regarding administrative burden were not addressed by the change. B: In Part 2.3, in the measures, the

wording change from “initially upon the effective date of the standard” to ”prior to the effective date of the standard” implies that evidence generated prior to the effective date of the standard can make the difference between complying or not complying with the standard. This leads to inadvertently requiring entities to do something prior to the effective date of the standard in order to comply. The new wording addresses our prior issue, but the Measures cannot reference activities that pre-date the effective date of the standard. Everything else looks OK.
No
No
R1: Part 1.4.2 requires the entity to verify that the “required controls and BES Cyber System availability” are not adversely affected. It doesn’t make sense to require the entity to verify BES Cyber System availability resulting from the change. Whenever there is an availability problem, it will be detected and acted upon when it occurs. A future availability problem cannot be verified before it occurs. It is suggested that the phrase “BES Cyber System availability” be removed from this requirement. Part 1.5.2 places an excessive administrative burden on the entities. R2: In Part 2.1, the language “not to exceed once every 35 calendar days” can be interpreted to mean that this cannot be done more than once every 35 days. This is obviously not the intent.
Individual
Andrew Gallo
City of Austin dba Austin Energy
No
No
No
CIP-003, R2 requires that low impact assets have a cyber security policy that addresses incident response to a BES Cyber Security Incident. CIP-008 deals with the creation of a cyber security incident response plan. Accordingly, CIP-008, Table R1, Parts 1.4 and 1.5 should include low impact assets. Additionally, please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
Yes
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
Yes
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
No
No
Please see the comments submitted by the Texas Regional Entity’s NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Group
Southern California Edison Company
Nathan Smith
Yes
Yes
Yes
SCE Comments to CIP-008-5 Please revise R3.4 to define “Technology changes” as changes to the internal environment that impact existing BES Cyber Systems.

Yes
Yes
Yes
No comments
No comments
Yes
Yes
Yes
SCE Comments to CIP-010-1 -R1.1 Please add the following flexibility to the “Effective Dates” Section as it is difficult to do accurately within the currently planned implementation window: “CIP-010-5, Requirement R1.1 shall become effective on the later of July 1, 2016, or the first calendar day of the 13th calendar quarter after the effective date of the order providing applicable regulatory approval. “ As we are sure the SDT is aware, the automation required to manage the base line configuration may impact Cyber Assets processor speeds, thus making the BES react more slowly.
Yes
Yes
SCE Comments to CIP-011-1 -R2.1 Please revise as follows: “…BES Cyber System Information (except redeployment in other high impact or medium impact BES Cyber Systems…” -R2.2 Please add the word “applicable” in front of “Cyber Asset” globally in the requirement.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
In R1 Part 1.5, the reference to forensics should not be part of the CIP-009 Standard
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI’s suggestions to strengthen the wording of this standard.

Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Yes
Yes
PGE takes cyber security very seriously, especially as it relates to the critical infrastructure necessary to maintain the continuing reliable operation of the Bulk Power System. PGE supports the important work of the Standards Drafting Team, along with other contributors and stakeholders who have assisted in the development of the proposed Version 5 standards. With that said PGE supports the standard as indicated by the responses above. PGE also agrees with EEI's suggestions to strengthen the wording of this standard.
Individual
Brian Evans-Mongeon
Utility Services Inc.
Yes
Yes
Yes
No Comments
No
Yes
Yes
Utility Services supports the comments made by MMWEC for CIP-009-5 T1, Part 1.5.
No
Yes
Yes
Utility Services supports the comments made by MMWEC in their Comments regarding CIP-010-1 R2.
Yes
Yes
Utility Services supports the comments made by MMWEC in their Comments for CIP-007-5 R2.1 and R2.2.
Individual
John Allen
City Utilities of Springfield, MO
No

No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
Yes
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
No
No
City Utilities of Springfield, Missouri would like to thank the drafting team for the tremendous amount of work it is putting into the development of this standard. We agree with the comments from SPP and APPA and believe the requirements are getting close to being acceptable for those cyber systems that could cause a significant impact to the BES. However, we cannot support this Standard due to the onerous requirements for a small entity's Control Center that are considered a threat to reliability due to their connectivity to High Impact Control Centers. We could support a standard that has programmatic requirements for these small Control Centers. See our response to Comment Form A, question 3.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.

No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Calendar year and 15 months are mutually exclusive. This requirement should use the term "Annual" as applied in NERC CAN-0010. Further, the term Annual should be added to the NERC Glossary of Terms.
Group
Dairyland Power Cooperative
Tommy Drea
Yes
No
Yes
Please see MRO NSRF comments.
No
No
Yes
Please see MRO NSRF comments.
No
No
No
Please see MRO NSRF comments.
Yes
Yes
Please see MRO NSRF comments.
Group
Progress Energy
Jim Eckelkamp
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Comment: Need to change the definition for Cyber Security Incident Progress Energy agrees with EEI comments with the modified and additional comments below: Original: Any Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity. Proposed: Any

Cyber Security Incident that has compromised or disrupted the operation of the BES and requires reporting per EOP-004. R2= Comments: Remove the word “BES” from the Requirement to be consistent with R1. Remove the words “lessons-learned report that includes a” from the Measures because the following items do not necessarily fall into the lessons learned category. Add a 2nd Measure “OR documentation from an actual Reportable Cyber Security Incident” as an alternative to the listed evidence. R3= R.3.2 Comment: Requirement - Clarify as follows “Maintain a current and up-to-date Cyber Security Incident Response Plan that (1) includes or references, as appropriate, documentation of any lessons, if any that may have been learned in connection with a Cyber Security Incident test or actual incident response performed pursuant to CIP-008-5 R2, within 90 days of the performance of such test or actual incident response; and (2) includes changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” Comment: Measures - Clarify as follows: “Evidence may include, but is not limited to, a dated, revised Cyber Security Incident Response Plan(s) that (1) includes or references, as appropriate, dated documentation of lessons learned, if any, associated with tests of or actual responses using the Cyber Security Incident Response Plan(s), within 90 days after completion of such test or actual incident response; and (2) reflects changes to roles or responsibilities, Cyber Security Incident response groups or individuals, or technology, within 90 days of such change.” R3.3 & R3.4: Remove these requirements as they are now incorporated into the proposed R3.2.
No
No
No
Progress Energy agrees with EEi comments with the modified and additional comments below 1. R3: In Order 706, paragraph 731, FERC stated “We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective.” We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: “Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: “Evidence may include, but is not limited to: 1) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; 2) dated emails, newsletters, training or other communications regarding the plan updates.” R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: “Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities.”
Comments: In all measures section remove the term “…but not limited to…” In “Guidelines and Technical Basis” section, list specific FAQs and CIPC guidelines that are applicable. Remove “Associated…Systems” from R1-R3 because Order 706 does not require them.
No
No

No
Progress Energy agrees with EEI comments with the modified and additional comments below R1= Comment: R1 Requirement - is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Comment: R1 Requirement remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4 Comment: R1.4 - Applicability - : Remove “High Impact” Rationale: it is repetitious with R1.5. Comment: R1.4 Requirement – There is no time requirement, but there wasn’t one in previous versions either. R2= Comment: R2.1 – Requirement - this is a borderline show stopper – will be burdensome and nothing gained from it except a lot of TFE paperwork to track Proposed: Recommend removing requirement R3= Comment: R3.1 & R3.4 – Applicability- Add “with External Routability” to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets Original: R3.1 - Requirement - At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls identified in CIP-005, CIP-006, and CIP-007 are implemented correctly and operating as designed. Proposed: At least once every calendar year, not to exceed 15 calendar months between assessments, conduct a paper or active vulnerability assessment to determine the extent to which the cyber security controls are implemented correctly and operating as designed. Original: R3.2 Requirement - Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment (or in a production environment where the test is performed in a manner that minimizes adverse effects) that models the baseline configuration of the BES Cyber System in a production environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. Proposed: Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment. If a test environment was used, document the differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments.
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Comment: R1.3 - Requirement & Measure - Change language time frames by removing “at least” and replacing with “once each calendar year or a period not to exceed 15 months”. R2= Comment: R2 uses the term “chain of custody” in several places. This is a legal term that relates to evidence, and is not appropriate in the CIP standards. EEI strongly suggests replacing it with “possession” or “control”. Comment: R2.1 – Requirement - In parenthetical text in change to read “(except for reuse in other high impact…)” for clarity. Additional Comments Comments: In all requirements, remove references to systems & assets and rely on the applicability column to specify applicability. In all measures sections in all standards and requirements remove the term “…but not limited to…” The default should be an “or”, and any “and” should be explicit. Rationale: these are examples only. Using the “limited to” language creates confusion about whether they’re necessary or sufficient. Applicability for all requirements should be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity” Several requirements use the terminology “BES Cyber System Information”, however this creates an inconsistency with all the “Associated…” assets in the Applicability column. Suggestion is to leave the applicability in that column, and don’t name asset/system types in the requirement. The length of the “Applicability…” column title can cause confusion about the systems/assets that are within scope. Suggest changing the column heading to “Applicability”.
Individual
Jennifer White
Alliant Energy
Yes
No
Yes
Overall it seems as if the standards writers are attempting to work out some subjectivity and ambiguity issues in regards to establishing sufficiency in meeting the requirements of the standards.

We do not believe that they have fully resolved these issues. Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Many requirements, if changed in accordance with our sometimes minor verbiage proposals, would be a “Yes.” [R2.2] – VSL must change for this such that it is not a violation if the incident response plan is not followed for an actual event. The requirement to document deviations is sufficient to meet the intended goal of ensuring the currency of the plan and updating it to reflect things discovered during actual incidents or drills. [R 3.1] – Suggest striking “and update” to IR plan review. It is possible that the plan is found sufficient after the review and would not require an update. Suggest verbiage “update, if necessary.” [R3.5] – Suggest striking “distribute”. What constitutes distribution? Suggest retaining “notification” approach. Distributing CIP protected data could pose technical issues, especially outside vendors. Notification, as long as the vendor had access would eliminate the need to actually distribute the plan to affected individuals. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs.
No
No
Yes
Comments: Once again it is straightforward to see the objectives the drafters are trying to accomplish, but the reality of this level of descriptiveness and compliance thereof, would be disruptive and prohibitive. Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. [R1] – The standard isn’t clear whether the recovery plans are for recovery of the asset, system, or function? Please clarify. Recommendation – the recovery should be for the function to link appropriately with the purpose of the CIP Standards. Otherwise, system is the lowest level of granularity that remains in alignment with the proposed BES Cyber System methodology. [R1.4] – Recommend striking associated physical access control systems and associated electronic access control systems from the applicability section. The wording of the requirement is unclear. What constitutes “initial,” “verification,” or “ensure the process completed successfully”? Suggest prescriptive wording if these terms are to be used. The current draft verbiage leaves too much up to the subjective interpretation of the auditor, and, if intended to be a daily or weekly check, could be administratively burdensome. Proposed Verbiage to align with FERC order 706: “Within the capabilities of the backup system and upon completion of a significant production change within a BES Cyber System, such as adding a new form of hardware or significant new software, data essential to BES Cyber System recovery that is stored on backup media shall be verified at the time the backup is created. Verification means the automated process typically incorporated into the automated backup process validates the bit count or similar technical function.” [R1.5] – Without tying this requirement to a Cyber Security Incident, there will be no forensic value in retaining the data if the event was not related to any malicious attempt. Proposed Verbiage: “Processes to preserve data, except for CIP Exceptional Circumstances, for analysis or diagnosis of the cause of a Cyber Security Incident that triggers activation of the recovery plan(s).” [VSL] These are appropriate. [R2.1] - Are the tests specified in R2 required for each cyber asset, cyber system, or each plan? In other words, does an entity need to do a “full operational exercise” on all systems, or is a representative sampling sufficient? [R2.2] – Is this in reference to the applications and other binaries used to restore or the actual plan itself? Suggest clarification. [Proposed Verbiage] “Validate the integrity of the stored backup information at least once per calendar year to ensure that the information is useable and is compatible with current system configurations.” [R2.3] – Is this requirement implying the need for a bare-metal restore for all CIP assets? Doing so would be cost-prohibitive and potentially jeopardize the stability of the BES. Some CCAs utilize a “standby” system for testing. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R3.4] – Once again the use of the word “distribution”. If I notified a vendor of an update to

the plan stored in CIP protected area, it would achieve the objective without the burden of any CPI issues in its “distribution”. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
No
No
No
Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. [R1.1] Recommend striking the applicability component of the main requirement. Applicability should be limited to the applicability column. [R1.1.3] – Proposed verbiage: “Any custom compiled software”. [R1.4] – Propose striking 1.4.1 to eliminate speculation or an implicit requirement to have a testing environment outside of 1.5. Instead, the CIP-005, CIP-006, and CIP-007 list should be moved to 1.4.2. This strike also removes the inflexibility as it relates to emergency change that exists in the current draft verbiage. In the absence of striking 1.4.1, recommend adding the CIP Exception Circumstances verbiage to 1.4 to allow emergency changes necessary to ensure operability/reliability. For those circumstances, 1.4.2 should suffice. If the intent of 1.4.1 is to expand the scope to include an understanding of potential impact outside of the existing baseline, this can be achieved without 1.4.1 with proposed verbiage: For a change that deviates from the existing baseline configuration or may have an impact on controls implemented for CIP-005, CIP-006, or CIP-007: and then skip to 1.4.2. [1.5] Recommend changing “where technically feasible” to “Where test environments exist” [VSL Recommendation] This VSL is written as a zero tolerance violation, even to the extent of indicating “any” undocumented change is a violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R2.1] – Recommend replacing “technically feasible” with “Within the capabilities of the system or network configuration.” Recommend striking the associated systems and cyber assets and leaving this to High Impact BES Cyber Systems with External Routable Connectivity. This also exceeds FERC 706, so we recommend increasing the interval of change detection to an annual or quarterly verification, because a manual process of verifying the baseline will be prohibitively administratively burdensome. Also, ports and services are an annual requirement, but they are also included in the baseline configuration here. This would require a validation of logical network accessible ports on a monthly basis and not tied to significant change. This creates a conflict within the standard. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria. [R3] – What is the definition of an “active vulnerability assessment”? What would be considered an appropriate infeasibility for performing such a test? Would the entity need to perform an “active vulnerability assessment” on all systems, or is a representative sampling sufficient? Recommend striking “CIP-006” from the list of cyber security controls assessed, as this is duplicative of the testing and maintenance requirement but increases the interval to annual instead of every 24 months. [R3.2] Recommend replacing “where technically feasible” with “Where a test environment exists or allowable within the operational risk of the production environment…” [R3.4] Recommend changing “planned date” to “estimated timeframe.” [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ

results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
Yes
Yes
Alliant Energy voted “Yes” on this requirement but still suggest adjustments per the suggestions herein: [R1.1] Recommend striking the first bullet in the Measures or changing it to indicate that a label of “confidential” is sufficient. The current measure is phrased such that it requires information to be labeled as CIP information, instead of just confidential. This increases the chances that someone will know how to use it maliciously if they do get unauthorized access to it. Suggest legacy verbiage indicating a classification in alignment with “confidential.” The current verbiage did not prevent organizations from assigning a “CIP Confidential” label to documentation or preclude a protection program that had only one level of protected information. [VSL Recommendation] This VSL is written as a zero tolerance violation with respect to the failure to implement even one action plan. Recommend, instead, that they be structured such that a Severe is the lack of a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. [R2.1 and 2.2] Recommend striking “chain of custody” to avoid connotations associated with legal definitions of this term that should not apply here. If the intent is to ensure positive control of the device until the information is removed, the phrasing should be in alignment with that. This phrasing should also allow secure methods of transport to the vendor if that is required within support contracts. [VSL Recommendation] This VSL is written as a zero tolerance violation. Recommend, instead, that they be structured such that a Severe is the lack of a program or the failure to implement a program; High is the lack of a way to detect and mitigate issues; Medium is that issues were detected but not mitigated; Low is that the issues were mitigated but preventative action was not taken. This is in alignment with the FFT process and encourages entities to employ results-based/performance-based programs. Additionally, VSLs should line up with the words in the requirement, itself, rather than create additive responsibility or criteria.
Individual
Tracy Richardson
Springfield Utility Board
No
Yes
No
SUB is concerned that the Requirements of CIP-008-5 create potential conflict with the Requirements of EOP-004-2. The development of the two Standards appears to be in parallel with one another, rather than working together. SUB recommends more coordination between the Version 5 CIP SDT and the EOP-004-2 SDT. SUB understands CIP-008-5 to be the “Incident Response Plan” and EOP-004-2 requires the development of an “Operating Plan for Event Reporting.” However, CIP-008-5 Table R1, Part 1.1 requires a process to “identify, classify, and respond to BES Cyber Security Incidents” while EOP-004-2 R1.1 requires; “A process for identifying events listed in Attachment 1.” SUB recommends the SDT revise the CIP-008-5 Requirement and Measure in Table R1, Part 1.1 to remove the terms “identify” and “classify.”
Yes
Yes
Yes
No
No
No
The definition of the term “configuration” is unclear. Configuration is not clearly defined in the Glossary of Terms Used in NERC Reliability Standards, Definitions of Terms Used in Version 5 CIP Cyber Security Standards, nor in the CIP-010-1 Cyber Security – Configuration Management and

Vulnerability Assessments Standard. Are “configuration management”, “configuration change management”, and “asset management” intended to be synonymous in the way they are used in the CIP-010-1 Standard? Configuration is only mentioned in terms of “security configurations”. SUB recommends that a specific definition be provided for Configuration, Configuration Management, Configuration Change Management, and/or Asset Management. Perhaps, based on the extensive changes to definitions in Version 5 of the CIP Standards, it would be appropriate to create a CIP-specific glossary of terms used in the CIP Standards. SUB recommends that the development of NERC Standard CIP-010-1 be a separate effort from the development of CIP Version 5 Standards.
Yes
Yes
Group
ACES Power Marketing
Jason Marshall
Yes
No
No
(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-008-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) In regards to Question 1 (CIP-008-5 R1): In the Rationale section it says, “Once the severity of an event or events rises to the level of becoming a Reportable Cyber Security Incident, NERC EOP-004 directs further external reporting actions and timing requirements.” The Guidelines and Technical Basis section for R1 under the Application Guidelines states, “The reporting obligations for Reportable Cyber Security Incidents are found in EOP-004-2.” In reading through EOP-004 it is still not clear how the two standards are to work with one another for reporting Cyber Security Incidents in regards to whom the report should be communicated. CIP-008-5 R1.5 states, “Internal groups or individuals and external organizations that should receive communication of the Cyber Security Incidents.” The Measure for CIP-008-5 R1.5 states that, “Evidence may include, but is not limited to, dated Cyber Security incident response process(es) or procedure(s) that list internal groups or individuals … and external organizations (e.g., law enforcement, ES-ISAC, software vendors, other affected entities) that should receive communication.” The Measure gives examples of entities that should receive communication. Is it up to the Responsible Entity to figure out to which external parties they should report Cyber Security Incidents? The drafting team should consider if a minimum list of required external entities is necessary to ensure consistent reporting and consistent auditing. (4) In regards to Question 2 (CIP-008-5 R2): Requirement R2.2 needs to be clarified. It reads, “Use the incident response plan under Requirement R1 when responding to or performing an exercise of a Reportable Cyber Security Incident.” This sentence when grammatically dissected says, “Use the plan when responding to an exercise or when performing an exercise…” We believe the intent of the SDT was to say, “when responding to a Reportable Cyber Security Incident or when performing an exercise of a Reportable Cyber Security Incident response plan.” Please re-phrase for clarity. (5) Regarding Question 2 (CIP-008-5 R2): The Rationale box and Part 2.2 uses the term “incident response plan” in place of “Cyber Security Incident response plan” as identified in Requirement R1. For consistency and clarity, we recommend using the more formal “Cyber Security Incident response plan” from Requirement R1. (6) Regarding Question 2 (CIP-008-5 R2): Part 2.1 states that the responsible entity is to test the BES Cyber Security Incident response plan. It indicates that response to an actual Reportable Cyber Security Incident would meet the requirement. Because response to an actual Reportable Cyber Security Incident would be an exercise of the response plan and not a test, we suggest changing “Test” to “Exercise”. (7) In regards to Question 3 (CIP-008-5 R3): The main requirement R3 is very similarly worded to the main Requirement R2. R2 focuses on testing and exercising the plan (implementation). R3 focuses on reviewing and updating the plan. R3 should be re-worded to better align with the objective. The Rationale for R3 states that “sufficient reviews, updates and communications” are conducted. To capture this, alternative language could be, “Each Responsible Entity shall review, update and distribute its documented Cyber Security Incident

response plan(s) to collectively …" Furthermore, this would make the requirement more consistent with the parallel requirement CIP-009-5 R3. (8) In regards to Question 3 (CIP-008-5 R3): The use of the word "within" throughout the R3 sub-requirements is confusing when used to reference number of days. One meaning of "within" is "inside a boundary." This could be interpreted as inside 30 calendar days but not including the 30th day. The meaning of "within" in the context of the requirements is "not beyond" or "not exceeding." Why not simply replace "within" with "does not exceed" to avoid confusion? In R3.1 "not to exceed 15 calendar months between reviews" is pretty clear. We recommend using similar language in R3.2 – R3.5 and the associated VSLs. (9) In regards to Question 3 (CIP-008-5 R3): Requirement R3.2 says to, "Document any lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days…" The Measure states that, "Evidence may include, but is not limited to, dated documentation of lessons learned, if any…" If there are no lessons learned, what is the Responsible Entity obligated to do to comply with the requirement? Is documentation stating there were no lessons learned from the incident sufficient? (10) In regards to Question 3 (CIP-008-5 R3): In the VRF/VSL section for R3, the words "within 30 and less than 60 calendar days" is very confusing. Using "and" means both conditions must be true. Anything within 30 days is automatically going to be less than 60 days so the phrase is redundant. Does the SDT mean to say, "greater than 30 but less than 60 calendar days?" (11) In regards to Question 3 (CIP-008-5 R3): The sub-requirement references in parentheses for the R3 VSLs are not represented correctly. For example, for the Lower VSL, the sub-requirement reference is to R3.4. It should be R3.5 since R3.5 requires the distribution of updates. All of the references in the VSLs for R3 need to be corrected. (12) In regards to Question 3 (CIP-008-5 R3): In the Guidelines and Technical Basis section for R3, the second sentence says, "There are two requirement parts that trigger plan updates: (1) lessons learned from Part 3.2 and (2) organizational or technology changes from Part 3.4." Isn't there a third requirement that would also trigger a plan update? R3.1 says, "Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews." The calendar year review would also trigger a plan update while not necessarily meeting the criteria of R3.2 or R3.4. Simply revising the date the plan was reviewed is technically an update. An erratum change would also qualify as an update. (13) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.

No

Yes

No

(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-009-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 5 (CIP-009-5 R1): The drafting team should develop application guidelines for these requirements. At the very least, the reference to the FAQs and CIPC Guidelines should be more specific with links to each guideline and FAQ. (4) Regarding the VSLs for CIP-009-5 R1: An additional gradation has been added, which is an improvement, but since there are five parts to R1, having four VSLs based on gradations of the number of parts missed would be a further improvement. (5) Regarding Question 6 (CIP-009-5 R2): Parts 2.1 and 2.3 state that the responsible entity is to test the BES Cyber Security Incident response plan. Both indicate that response to an actual Reportable Cyber Security Incident would meet the requirement. Because response to an actual Reportable Cyber Security Incident would be an exercise of the response plan and not a test, we suggest changing "Test" to "Exercise". (6) Regarding Question 6 (CIP-009-5 R2): Part 2.2 should clarify that actual recovery of a BES Cyber System using the backup media meets the requirement. (7) Regarding Question 7 (CIP-009-5 R3): Part 3.4 needs to be modified to be consistent with Part 1.2 of Requirement R1. Part 3.4 requires the recovery plan to be distributed to "each individual responsible under R1.2". First, R1.2 needs to be changed to Requirement R1, Part 1.2 to be consistent with language NERC submitted to the Commission describing the use of parts in place of sub-

requirements. Second, Requirement R1, Part 1.2 was modified to remove the need to identify specific individuals in the recovery plan. This was done to eliminate the documentation challenges associated with maintaining recovery plans every time there is a personnel change. We suggest replacing “each individual” with “responders” from Part 1.2. Third, “distribute” should be changed to “make available” or “notify”. Distributing implies that the actual recovery plans should be communicated (i.e. email attachment, hand delivered). All that is needed is for the responders to be made aware an update has occurred to a recovery plan. (8) Regarding the VSLs for CIP-009-5 R3, the words “within 30 and less than 60 calendar days” is very confusing. Using “and” means both conditions must be true. Anything within 30 days is automatically going to be less than 60 days so the phrase is redundant. Does the SDT mean to say, “greater than 30 but less than 60 calendar days?” (9) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.
No
No
Yes
(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-010-1 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 9 (CIP-010-1 R1): Removal of BES before Cyber Asset in Part 1.1 has the impact of greatly expanding the requirement. By definition a Cyber Asset is any “programmable electronic device”. Thus, computer systems that have absolutely no impact on the Bulk Electric System could be pulled into the requirement. We recommend not only adding BES back to Cyber Asset but also clarifying that the requirement only applies to applicable BES Cyber Assets. Thus, we suggest replacing “Cyber Asset” with “applicable BES Cyber Asset” throughout Part 1.1 and its associated measure. (4) Regarding Question 9 (CIP-010-1 R1): The timeline established for Part 1.3 conflicts with some of the timelines established in CIP-005-5 and CIP-007-5. For example, Part 3.3 in CIP-007-5 requires an update of “malicious code protections” at least once every 35 days. CIP-010-1 R1 Part 1.3 requires updates to the baseline configuration within 30 days which would also included updating “malicious code protections”. We suggest removing CIP-005 and CIP-007 as a reference to eliminate this issue. (5) Regarding Question 9 (CIP-010-1 R1): Part 1.3 presents opportunities for double jeopardy by including references from CIP-005 and CIP-007. If a change to the ports configuration is made but documentation from CIP-005 and CIP-007 is not updated, CIP-010-1 R1, CIP-005 and CIP-007 could all be violated simultaneously. (6) Regarding Question 9 (CIP-010-1 R1): Part 1.4 is partially redundant, unnecessary and completely ambiguous. It essentially says that the responsible entity needs to identify the “required cyber security controls identified in CIP-005, CIP-006 and CIP-007” in Part 1.4.1. First, they are not controls but requirements and should be referred to as such. Second, CIP-005, CIP-006, and CIP-007 are standards that should stand alone without the need to have another requirement say that they should be implemented. Thus, we are left unsure what the intent of this requirement is. (7) Regarding Question 9 (CIP-010-1 R1): To ensure the statement in parentheses in Part 1.5.1 has the same impact as the rest of the requirement, the parentheses should be removed. The statement with the parentheses is not an explanatory statement but actually modifies the requirement. (8) Regarding Question 9 (CIP-010-1 R1): The Measure for Part 1.3 should be clarified to say “within 30 calendar days” to be consistent with the Requirement. (9) Regarding Question 9 (CIP-010-1 R1): Part 1.4 should be given an exclusion for CIP Exceptional Circumstances. (10) Regarding Question 10 (CIP-010-1 R2): Part 2.1 conflicts with the application guidelines. The application guidelines explain that periodic monitoring is included in the requirement to allow for monitoring of BES Cyber Assets that don’t have the capability to be monitored continuously. Thus, a responsible entity could manually check the baseline configuration at least once every 35 days. While a periodic manual check would always seem to be technically feasible, it may not be practical based on staffing levels. Thus, it is not clear if the clause “where technically feasible” applies to both the continuous and periodic monitoring. (11) Regarding Question 10 (CIP-010-1 R2): To ensure the statement in parentheses in Part 3.2 has the same impact as the rest of the requirement, the parentheses should be removed. The statement with the parentheses is not an

explanatory statement but actually modifies the requirement. (12) Regarding Question 11 (CIP-010-1 R3): Part 3.3 appears to be missing “and” after the parenthesis. Without the parenthetical, it should read “Except for CIP Exceptional Circumstances and like replacements and prior to adding a new Cyber Asset…” (13) In regards to Question 11 (CIP-010-1 R3): Part 3.4 does not specify a deadline for documenting the results of the assessments and the action plan to remediate or mitigate vulnerabilities. We suggest a 30-day limit for documentation associated with this requirement. Otherwise, debates could arise between the registered entity and regional entities on what constitutes timely compliance. Along with adding a deadline to the actual requirement, we recommend also adding levels of VSL gradation for not meeting the 30-day limit. (14) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.
Yes
No
(1) In regards to the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (2) Regarding Section 4.2.4 Exemptions: This section was changed from the last posting to indicate the exemptions are for CIP-002-5. CIP-002-5 already has the same exact exemption language. Either this reference should be changed back to CIP-011-1 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (3) Regarding Question 13 (CIP-011-1 R1): There is a missing “or” after the first bullet of the measure. (4) Regarding Question 14 (CIP-011-1 R2): BES should be inserted prior to Cyber Assets in Part 2.2. Otherwise the requirement could be expanded to cover any computer or control system that does not impact the BES. Cyber Asset has a much different meaning than BES Cyber Asset. (5) Regarding Background Section 5: The third paragraph regarding measures has contradicting ideas. It states that a numbered list in the measure means that the evidence list includes all required items. However, the last sentence states that the measures serve to provide guidance and should not be viewed as all inclusive. Which is it? We support the latter.
Individual
Anthony Jablonski
ReliabilityFirst
CIP-008-5 1. VSL for Requirement R2 a. The last VSL under the “High” category seems to be erroneous. It states “The Responsible Entity does not document deviations, if any, from the plan during a test or when a Reportable Cyber Security Incident occurs. (2.2)” though it does not relate to associated Requirement R2 Part 2.2 in any manner. ReliabilityFirst Recommends deleting this VSL. 2. VSL for Requirement R3 a. General comment – References to the Part numbers are incorrect for a number of the VSLs. For example, the “Lower” VSL has an incorrect reference to Part 3.4. The reference should be to Part 3.5. ReliabilityFirst recommends checking the references to the Part numbers to ensure accuracy. b. A VSL associated with Requirement 3, Part 3.1 is missing from the VSL table. Part 3.1 states: “Review and update each Cyber Security Incident response plan for accuracy and completeness at least once each calendar year, not to exceed 15 calendar months between reviews.” ReliabilityFirst recommends adding a VSL associated with Part 3.1.
CIP-009-5 1. VSL for Requirement R1 a. ReliabilityFirst believes the “Moderate” VSL has a typo. The “Moderate” VSL incorrectly states: “do not address all of the requirements.” Based on the gradation of other VSLs for R1, ReliabilityFirst believes this VSL should be modified to correctly state “do not address one of the requirements.” 2. VSL for Requirement R2 a. There seems to be a conflict between the first and second VSLs under the “Severe” category (the VSLs associated with Part 2.1 and Part 2.2). The VSL for Part 2.1 indicates “18 calendar months” and the VSL for Part 2.2 indicates “19 calendar months”. Even though these are separate Parts, the timeframes are of the same length in the requirement and ReliabilityFirst recommends these two VSLs be modified to be consistent. 3. VSL for Requirement R3 a. The first VSL under the “Moderate” category has an incorrect parenthetical reference to Part 3.1. This VSL is actually associated with Part 3.2. b. The second VSL under the “High” category has an incorrect reference to Part 3.2 within the VSL itself. ReliabilityFirst recommends modifying the VSL as follows: “…60 calendar days after the documentation required by R3 Part 3.1. (3.2)”

CIP-010-1 1. VSL for Requirement R1 a. ReliabilityFirst recommends adding a reference to the associated “Part” in which each VSL is related to. It is very hard trying to trace the VSL back to the associated Part number. For example, if a Responsible Entity failed to comply with Parts 1.1 or 1.5, it is unclear which VSL they would fall under. Also, based on FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. New terminology in the VSLs should be avoided that doesn’t already exist in the associated requirement. 2. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “The Responsible Entity has not implemented a configuration monitoring process” to be consistent with the language in Requirement R2. Also, there is no mention of the Responsible Entity monitoring continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (per Part 2.1) in the VSLs. ReliabilityFirst recommends the following: “The Responsible Entity has not implement one or more documented processes to monitor continuously or periodically, not to exceed once every 35 calendar days, for changes to the baseline configuration (as defined per CIP-010 R1, Part 1.1). 3. VSL for Requirement R3 a. All the VSLs for Requirement R3 start off with the language: “The Responsible Entity has established one or more documented” while Requirement R3 requires the Responsible Entity to “…implement one or more documented processes…”. To be consistent with the requirement, ReliabilityFirst recommends the VSLs should start off with the following language: “The Responsible Entity has implemented one or more documented processes…” b. ReliabilityFirst recommends adding a reference to the associated "Part" in which each VSL is related to. Without referencing the associated Part number, it is very hard to trace the VSL back to the associated Part number. Also, based on FERC Guideline 3, VSL assignment should be consistent with the corresponding requirement and should not expand on, nor detract from, what is required in the requirement. New terminology in the VSLs should be avoided that doesn’t already exist in the associated requirement.
CIP-011-1 1. General comment for VSLs for Requirements R1 and R2 a. ReliabilityFirst recommends adding a reference to the associated “Part” in which each VSL is related to. Without referencing the associated Part number, it is very hard to trace the VSL back to the associated Part number.
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Comments: In R2, replace “chain of custody” with “possession” or “control” as chain of custody is a legal term related to evidence
Group
SPP and Member companies
Lesley Bingham
Yes
Yes
Yes

Part 3 can be shortened to two sub-requirements by leaving Part 3.1 as is and adding the following as Part 3.2 “For any required change to the recovery plan (due to deficiencies or lessons learned from recovery plan tests or actual incident recoveries, or changes in roles, responsibilities, or technology), update the recovery plan and distribute updates to each individual responsible under R1.3 within 60 calendar days”.
Yes
Yes
Yes
Yes
Yes
Yes
If an entity is building systems with a documented baseline and monitoring it closely, the vulnerability assessment prior to deployment will have no benefit. Additionally, it will be difficult (not to mention expensive) to establish a production-like environment which would produce an accurate vulnerability assessment.
Yes
Yes
Group
IRC Standards Review Committee
Christine Hasha
Yes
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding the combination of CIP-008-5 Requirements 3.2 and 3.3 under question 4.
Yes
Yes
Yes
The IRC requests combining Requirement R3.1 and R3.2 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s).
The IRC requests combining Requirement R3.1 and R3.2 and allow 60 calendar days to document identified deficiencies or lessons learned, and update the recovery plan(s).
Yes
Yes
No
The IRC believes that CIP-010-1 Requirement 3.1 could be seen as redundant to 1.3. A vulnerability assessment should not be a compliance check of the controls listed in CIP-005, CIP-006, and CIP-007. Requirements 3.3 and Part 3.4 define what is meant for a vulnerability assessment. This may not be sufficient to address current vulnerabilities. The IRC requests clarification of whether the vulnerability assessment is to check against known vulnerabilities or simply a compliance check of the CIP requirements. The IRC requests that CIP-010-1 Requirement 3.2 have Associated Electronic Access Control or Monitoring Systems and Associated Protected Cyber Asset added to the applicability.
Yes
Yes
Individual
Scott Kinney
Avista

See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
See comments provided by EEI
Individual
Gregory Campoli
NYISO
No
No
No
• R1 – Concerns EOP-004-3 is not accepted and the reference between future and requirement may not link well. Should not assume EOP-004-3 is approved. • R2 Part 2.1 Recommend changing the first bullet from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents • Recommend updating R2 Part 2.3 since the existing language does specify a retention period. • Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security Incident response plan will not need updating
No
No
• R1.5 – Recovery plans are for restoring service. ITIL incident management is for restoring service which is the priority for BES support. Root cause analysis is where forensics would be considered and could really detract from BES operations. Priority is to Availability impact for BES cyber systems so don’t introduce conflict with forensics in the requirements. Best practice should be forensics. • R2.3 may have bookends on periodic requirements in the requirement so please clarify.
No
No
No
• R1 Please clarify what “intentionally installed software” covers as systems come with applications and device drivers that may include executable and DLL files. • Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc” instead of “device drivers, DLL, applications included in an operating system or package, etc?” • Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? • Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? • In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part) • Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? • In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways • In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity • For R2 Part 2.1, recommend the previous version 5 words since this updated Part is not understandable • Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? • In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations • Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment • Request

clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. • Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. • Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” • Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low” • Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”
Yes
No
• R2 Recommend moving the second paragraphs of R2 Parts 2.1 and 2.2 into a new Part 2.3 for clarity.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
Yes
No
Yes
Yes
R1.4 states backup media shall be “verified initially after backup,” the terms verified initially are vague. Many automatic backup systems run a series of backups at different times and report if the backup was successful. FEUS recommends the drafting team revise R1.4 to state “verified the backup was successful by the end of the next business day.” FEUS recommends revising to align with the measures, “Information essential to BES Cyber System recovery that is stored on backup media shall be confirmed to ensure that the backup process completed successfully.” Additionally, the evidence required to demonstrate with R1.4 would be burdensome to maintain for three years since most entities run multiple backups on multiple systems at different periodicities. FEUS recommends changing the data retention to R1.4 to 90 calendar days.
Yes
Yes
Yes
Yes
Yes
See comments submitted with CIP-004; CIP-004-5 R6.1.3: This should be removed – the protections should be included in the information protection program provided by CIP-011-1. It is noted the measures include, “and access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” FEUS is concerned that electronic information may be stored in an electronically secured location (aka laptop or encrypted/protected USB) but the physical location may be very mobile in that ‘physical’ location varies. In additional, even printed material may be ‘mobile’. For example, printed copies physically transferred from a Primary Control Center to a Backup Control in which the physical location may be a briefcase in the direct control of someone with access. This type of situation is better handled by an individual’s information protection program rather than the Access Management Program. CIP-004-5 R6.4 should be removed from this Requirement included in the information protection program provided by CIP-011-1. At a minimum, the SDT should clarify what is meant by physical access. See comments for CIP-004-5 R6.1.3 – the physical location of printed or electronically stored information may not be stationary and may be

impossible to control based on the circumstance. This would be better defined in the Information Protection Program to allow flexibility. CIP-004-5 R6.7: See comments for 6.1.3 and 6.4 CIP-004-5 R7.3: FEUS feels this would be better defined by an entities Information Protection Program; see comments in R6 regarding the physical location of System Information

Individual

Maggy Powell

Exelon Corporation and its affiliates

No

No

No

CIP-008-5, R1: The examples in M1.4 are confusing relative to R1.4. Post-incident analysis does not seem to track with the requirement for incident handling procedures. Recovery is covered in CIP-009. It's conceivable that an entity may have one document to demonstrate evidence for multiple requirements associated with incidents; however, the examples imply that recovery documentation would suffice as evidence for the incident handling procedures. Please remove "(e.g., containment, eradication, recovery, post-incident analysis)" from M1.4. CIP-008-5, R2: The defined term for Cyber Security Incident does not include BES and shouldn't be added in R2.1. Please remove "BES" from R2.1 to read: "Test the Cyber Security Incident response plan(s) …" CIP-008-5, R2: Also, for consistency, R2.2 should spell out Cyber Security Incident. Update R2.2 to read: "Use the Cyber Security Incident response plan …" CIP-008-5, R3: Two bullets in M3.5 are not cited as forms of evidence. Please update M3.5 to read: "Evidence of distribution of updates may include, but is not limited to: - Emails; - Delivery receipts from USPS or other mail service; - Delivery receipts from electronic distribution system; or - Training sign-in sheets.

No

No

No

CIP-009-5, R1: M1.3 is missing an "and." For consistency with R1.3, M1.3 should read: "Evidence may include, but is not limited to, documentation of specific processes for the backup and storage of information…" CIP-009-5, R1: In R1.4, It is clearer to us for the terms "verified" and "initially" to be reversed in order. Please consider revising R1.4 to read: "Information essential to BES Cyber System recovery that is stored on back up media shall be initially verified after backup..." Even with the above proposed revision, R1.4 raises significant questions about what is intended by the terms “initially,” “verified” and “backup.” By extension, the compliance demonstration obligations under M1.4 also depend on the intended type of backup, the quantity of data and duration of record keeping. As currently written, CIP-009-5, R1.4 is unclear and could impose a compliance burden in terms of manpower and documentation to comply that overwhelming outweighs a benefit to reliability or security. We suspect that the intent is to ensure that the backup process works reliably and that verification would be satisfied by a confirmation of the completed backup process. As the SDT revisits R1.4, it may be useful to consider dropping the word “initially”. Further, we expect that the requirement obligation does not warrant recording daily or continual backups and a subset of data should be sufficient to demonstrate compliance. Depending on the intended “verification” and “backup” type, M1.4 may need to define "logs" as operational logs and thereby limiting the data retention to 90 days. Alternatively, set a number of backups, perhaps 10, as a level sufficient to demonstrate that the backup works reliably. Perhaps contributing to the confusion with R1.4 is that CIP-009-3 R5 called for an annual requirement for testing backup media and is no longer part of the standard or discussed in the rationale. We recognize that the proposal cites CIP-009-5, R1.4 as a new requirement; however, some discussion of the evolution may help further clarify the intent. CIP-009-5, R2: Relative to the R2 test requirements, please discuss what/how much information is intended for the test. A representative sample should be acceptable to demonstrate a test. CIP-009-5, R3: As in CIP-008, R3.5, two bullets in CIP-009, M3.4 are not cited as forms of evidence. Please update M3.4 to read: "Evidence of distribution of updates may include, but is not limited to: - Emails; - Delivery receipts from USPS or other mail service; - Delivery receipts from electronic distribution system; or - Training sign-in sheets.

No

Yes

No

CIP-010-1, R1: In R1.3.3 the use of the undefined term “custom software developed for the entity” does not clearly include or exclude user applied parameters used to configure core functions in a device’s standard software or firmware; relay settings are an example of this. As well, please discuss what may be grouped under R1.1.” CIP-010-1, R1: R1.1.2 should not have BES in front of Cyber Asset. Please revise R1.1.2 to read: "Any commercially available or open-sources application software (including version) intentionally installed on the Cyber Asset;" CIP-010-1, R1: More problematic in R1.1.2 is the term “intentionally.” Inclusion of this term raises the question of how to prove intentional or unintentional installation. For instance, if an entity installs commercially available software, but is unaware that the package also included java software, what are the obligations of the entity? We suggest removing the word intentionally so that R1.1.2 reads: "Any commercially available or open-sources application software (including version) installed on the Cyber Asset;" CIP-010-1, R1: A word order adjustment to R1.5.1 will improve clarity. Please consider revising R1.5.1 to read: "Prior to implementing any change in the production environment, test the changes in a test environment that models the baseline configuration (or in a production environment where the test is performed in a manner that minimizes adverse effects) to ensure that required cyber security controls are not adversely affected; and" CIP-010-1, R3: A word order adjustment to R3.2 will improve clarity. Please consider revising R3.2 to read: "Where technically feasible, at least once every 36 calendar months between assessments, perform an active vulnerability assessment in a test environment that models the baseline configuration of the BES Cyber System in a production environment (or in a production environment where the test is performed in a manner that minimizes adverse effects). ..." CIP-010-1, R3: As well, R3.3 is not clearly stated. Please consider revising R3.3 to read: “Prior to adding a new Cyber Asset, perform an active vulnerability assessment of the new Cyber Asset (except in CIP Exceptional Circumstances or when a replacement Cyber Asset is of the same type and same baseline configuration of the previous Cyber Asset).” CIP-010-1, R3: R3.4 does not clearly identify which vulnerability assessments correlate with the action plans. Please confirm that the action plans in R3.4 refer to the vulnerability assessments in CIP-010-1, R3.1, R3.2 and R3.3. Please consider revising to R 3.4 to read: "Document the results of the assessments conducted per CIP-010-1 R3, Part 3.1, 3.2 or 3.3 and the action plan to remediate or mitigate vulnerabilities identified in the assessments including the planned date of completing the action plan and the execution status of any remediation or mitigation action items."

No

No

CIP-011-1, General: The component obligations under CIP-011-1 are not clearly split into the requirement divisions. The table headers under R2 may be adding to the confusion as they are different for R2.1 and for R2.2. It appears that the general heading for the R2 tables should be Reuse and Disposal. Then the sub-requirements should breakout the requirements specific to BES Cyber Assets and Media respectively. R1 addresses information, but does not discuss disposal and destruction of information. R2 discussed disposal but does not discuss disposal of information. CIP-011-1, R1: Did the drafting team intend to include procedures for disposal and destruction under R1.2? Or does R2 cover the relevant measures for destruction and disposal? CIP-011-1, R1: M1.1 lists "Repository or designated electronic and physical location" as evidence. Please clarify how the repository demonstrates that documents are identified and BES Cyber System Information. It is important to clarify that while a repository may be a tool for BES Cyber System Information, all information within a repository may not automatically be subject to the restrictions associated with BES Cyber Security Information. CIP-011-1, R1: FYI - the reference to prior version under R1.2 refers to CIP-003-3, R5.3. This should perhaps be listed under R1.3 instead. CIP-011-1, R1: Is classification or determination of BES Cyber System Information a required part of the handling procedures for R1.2? CIP-003-4 specifically required classification of CCA information (CIP-003-4, R4. Information Protection —The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.) It’s not clear that classification or determination continues within CIP-011. CIP-011-1, R1: Part 1.2 Change Rationale states that the SDT removed the language “protect” information and replaced it with “handling” information to clarify that protection is required. To be more clear, should it be “One or more documented and implemented procedures for the protection and handling of BES Cyber System Information…”?

Group

CenterPoint Energy
John Brockhan
No
No
No
R1.5 – CenterPoint Energy recommends removing this requirement or alternatively, proposes that "Reportable" be added to Cyber Security Incident. R2.2 – CenterPoint Energy believes this requirement is too prescriptive as it relates to documenting deviations and recommends that the SDT remove "documentation of deviations" as deviations will be captured in lessons learned. R3.1 - CenterPoint Energy proposes the following alternative language to indicate annual requirements: “Once per calendar year but there should be no more than 15 months between activities." CenterPoint Energy also recommends that the SDT add "except in CIP Exceptional Circumstances” as also noted in the comments submitted by EEI. R3.2/R3.3 – CenterPoint Energy proposes that "if any" be added to the noted requirements. CenterPoint Energy also request that “with External Routable Connectivity” be added to the Medium Impact Applicability as also noted in the comments of EEI and NSRS. Guidelines & Technical Basis – CenterPoint Energy recommends that the guidance for Requirement 3 be updated to reflect changes to the requirement since the last formal comment period. CenterPoint Energy also agrees with the comments submitted by NSRS for this Standard.
No
Yes
No
R3.1 – CenterPoint Energy recommends that the SDT merge 3.1 and 3.2 and change the timeframe to 60 days as similarly noted in the comments submitted by EEI. CenterPoint Energy also agrees with the comments submitted by NSRS.
No
No
No
R1 - CenterPoint Energy believes that the changes to this requirement are too prescriptive and burdensome, particularly for the substation environment. The Company also recommends that this requirement and all of its sub requirements should not be applicable to Medium Impact Facilities as it is not a FERC directive to include such Facilities. The Guidelines and Technical Basis is also only targeted at Control Centers. R2.1 – CenterPoint Energy proposes that the SDT change the timeframe associated with this requirement to 90 days. R3.1 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. R3.4 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. CenterPoint Energy also generally agrees with the comments submitted by NSRS.
No
Yes
R1.1/1.3 - CenterPoint Energy recommends that the SDT add “with External Routable Connectivity” to the Medium Impact applicability for this requirement. CenterPoint Energy also agrees with the comments submitted by NSRS.
Individual
James Tucker
Deseret Power
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
No
Yes
R1.3 – DESERET POWER requests clarification regarding whether “deficiencies identified during the assessment” are considered violations of the standard. DESERET POWER believes these deficiencies should not be considered violations and requests that the SDT make this clear in the requirement language.
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Clarify that deficiencies found are not to be considered a violation.
Group
Seattle City Light
Pawel Krupa
General Comments: SCL does not support the approach proposed in version 5 of the CIP Standards, either as to fundamentals or details. Fundamentally SCL believes the v5 approach is flawed and will introduce significant compliance burden without ensuring cyber security for the BES. Detailed concerns remain as provided previously (please refer to comments submitted by SCL on January 6, 2012). Although today's enforcable CIP Standards share many of the flaws of v5, SCL believes industry would be better served by developing maturity around the existing Standards while developing a new, different approach to cyber security that is based on the established practices and theory of the information technology industry.
Individual
Steve Alexanderson P.E.
Central Lincoln

Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Yes
Yes
We disagree with 4.22 bullet three. Section 215 of the FPA states “The term ‘‘reliability standard’’…, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity.” Therefore, it is not permissible to write a reliability standard that requires the installation of a Transmission Protection System. We ask that bullet three be removed.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp support comments submitted by EEI.
Individual
John Tolo
Tucson Electric Power
Yes
Yes
Yes
TEPC agrees with EEI Comments: Change all instances of Medium Impact BES Cyber Systems to “Medium Impact BES Cyber Systems with External Routable Connectivity” for consistency with CIP-005, CIP-006, and CIP-007.
Yes
Yes

No
TEPC agrees with EEI comments: : R2.1: Modify the first part of the requirements language to read "Test a representation of the recovery plans(s) referenced in Requirement R1 once each calendar year or not more than 15 calendar months between tests except for CIP Exceptional Circumstances." Rationale: Reduce significant confusion. R2.2: a) Change the first 3 words of the requirement to read "Test representative information"., R3: In Order 706, paragraph 731, FERC stated "We believe that allowing 30 days to update a recovery plan is more appropriate, while continuing to allow up to 90 days for completing the communications of that update to responsible personnel. However, the Reliability Standards development process may propose a time period other than 30 days, with justification that it is equally efficient and effective." We believe that updates to the plan are not effectively in place until it has been communicated, and that it will be more efficient for entities to track one date rather than four date requirements included in draft 2. We propose consolidation of the four subparts of R3 into one subpart that ensures up-to-date recovery plans and communications within the 90 days required in FERC 706 but is less prescriptive and less of a documentation burden. Delete R3.2, R3.3 and R3.4 and use the following text for R3.1: "Update recovery plan(s) and communicate the updates within 90 calendar days of a test, actual recovery or changes that impact the ability to execute the plan. Updates from tests or actual recovery shall include lessons learned. R3 MEASURES: With the consolidated R3.1 requirement, the following is proposed for measures: "Evidence may include, but is not limited to: a) revised recovery plan(s) that include dated references to lessons learned from tests, actual recovery or changes that impact the ability to execute the plan; b) dated emails, newsletters, training or other communications regarding the plan updates." R3 VSLs: Replace the draft 2 VSLs with the following. Lower VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 90 and less than 120 days of the change, test or actual recovery. Moderate VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 120 and less than 150 days of the change, test or actual recovery. High VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 150and less than 180 days of the change, test or actual recovery. Severe VSL: The Responsible Entity has not completed updates and communications of the recovery plan within 180 and less than 210 days of the change, test or actual recovery. R3 GUIDANCE: Add the following to guidance: "Individuals responsible for activating and implementing a recovery plan should have information needed to recover their assets. R3 is meant to ensure recovery plans are up to date and available to individuals who need them. The following are examples of items that might require updates and communications within the 90 day timeline: * changes needed as a result of lessons learned from a test or actual recovery; * changes in roles and responsibilities."
No
Yes
Yes
TEPC agrees with the following comments from EEI: R1: remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4; 3) R2: remove Associated assets/systems from applicability because they go beyond Order 706. R1.1: Add "with External Routability" to Medium Impact BES Cyber Systems; 5) R1.4: Remove "High Impact" from Applicability because it is repetitious with R1.5. R3.1: a) Applicability: Add "with External Routability" to Medium Impact BES Cyber Systems and Associated Protected Cyber Assets.
Yes
Yes
Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Yes
No
Yes
R2.1 states that the entity is to test the recovery plan(s) every calendar year, not to exceed 15 months. R2.3 seems to be a facsimile of 2.1, yet adds a longer timeframe for compliance. We need clarification on the timeframes, as there may be overlap between the two activities. Furthermore, there needs to be clarification or additional guidance for the types of operational excercises the drafting team is requesting entities to perform per R2.3.
Yes
Yes
No
R3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. Furthermore, the term "Active vulnerability assessment" is not defined. Under the assumption that an "active vulnerability assessment" is the actual performance of an entities vulnerability assessment program, there are sufficient controls in place that would deem an "active vulnerability assessment" unnecessary, such as change management procedures. Therefore, we request that R3.3 be removed.
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.

No
Yes
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
No
No
Yes
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Yes
No
We thank the SDT for improvements to the draft standard, however, we still believe there is room for more improvement before voting affirmative. For specific concerns, please see the formal comments of ACES Power Marketing.
Group
Puget Sound Energy, Inc.
Tom Flynn
Yes
Yes
Yes
R3.2 states that "…lessons learned associated with a Cyber Security Incident test or actual incident response to a Reportable Cyber Security Incident within 30 calendar days after the completion of the test or actual incident response." While 30 calendar days would be sufficient time to document lessons learned from a test of the plan or a minor incident, there is the potential of larger or more complex incidents requiring considerably longer than 30 calendar days to accurately document lessons learned. Recommendation: Add language to the requirement to say that the CIP Sr. Manager or delegate is required to approve any lessons learned documentation that will exceed 30 days to complete.
Yes
No
No
(1) In the Measure for R2.2, the evidence required includes the "BES Cyber Systems that is stored on backup media when initially stored and at least once each calendar year…" PSE feels the wording suggests you have to test the backup media twice, and requests that the words "when initially stored" be dropped from the measure. This clears up any confusion on when the backup evidence must be tested "once each calendar year…". (2) In Requirement R3.2, when referring to "Update the recovery plan(s) based on any documented deficiencies or lessons learned within 30 calendar days", PSE feels that 3.3 is sufficient to tracking changes to the documentation based on implementations from the lessons learned. Applying lessons learned could require program, process and technology changes that may take several months to a year to implement. At which time documentation changes would then be updated according to Requirement 3.3. PSE recommends removing this requirement and clarifying the need for this updating in accordance to 3.1 and 3.3 respectively.
Yes
Yes
Yes
R1.5 states: "Where technically feasible, for each change that deviates from the existing baseline configuration…" The updated wording in R1.5.1 seems to remove any chance of a technical

infeasibility. Is a Technical Feasibility Exception (TFE) expected in cases where an entity cannot test in a test environment or cannot document that the test performed in a production environment is done in a manner that minimizes adverse effects? Suggestion: Remove “where technically feasible” since the new wording in R1.5.1 provides options for an entity to determine production environment tests that minimize adverse effects.
Yes
Yes
R2.1 – The measures state that evidence may include “Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information…” PSE requests clarity as to what form of record should be produced to provide evidence that action has been taken. Does the SDT believe that an attestation from the individual performing the action or a completed change control document would constitute sufficient evidence? R2.2 - The measures stat that evidence may include "Other records showing actions taken to prevent unauthorized retrieval such as encrypting, retaining in the Physical Security Perimeter;" PSE requests clarity as to what form of record should be produced to provide evidence that action has been taken. Does the SDT believe that an attestation from the individual performing the action or a completed change control document would constitute sufficient evidence?
Group
PNM Resources
Michael Mertz
No
No
No
See comment submission from EEI.
No
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
No
See comment submission from EEI.
No
No
See comment submission from EEI.
Individual
Scott Harris
Kansas City Power & Light
No
No
Yes
R1.2: The definition of reportable cyber security incident is unclear. DOE form 417 explains what must be reported. R2: Add “except for CIP exceptional standards.” To the requirement
No
Yes
Yes
R1.4: The only way to ensure that a backup was completed successfully is to restore data from a backup. Suggested change: 1.4 Incomplete or failed backups for information essential to BES Cyber System recovery shall generate alerts.

No
No
No
General: In all requirements sections, remove references to systems & assets and rely on the applicability column to specify applicability. R1: R1 is too prescriptive. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Remove Associated assets/systems from applicability because they represent an increase in scope from CIP v3/v4. R1.1-R1.4: Adjust requirement to require a baseline configuration for only devices that use a routable protocol. All devices will require entities to make increased financial and manpower investments to comply. It does not recognize the other controls for hardware or software changes, malware and virus defenses, or physical and electronic access controls to prevent unauthorized changes. Recommend that the CIP v3/v4 language replace 1.1-1.4, but specifically address the Order 706 requirements for malicious changes. Add “with External Routability” to Medium Impact BES Cyber Systems. R2: Remove Associatted assets/systems from applicability because they go beyond Order 706. R2.1: Adjust requirement to require a baseline configuration for only devices that use a routable protocol. All devices will require entities to make increased financial and manpower investments to comply. It does not recognize the other controls for hardware or software changes, malware and virus defenses, or physical and electronic access controls to prevent unauthorized changes. Remove Associated assets/systems from applicability because they go beyond Order 706. R3.2: Remove the words “that models the baseline configuration of the BES Cyber System in a production environment” after the parentheses. R3.3: Change the words “prior to adding” to “as part of the change prior to completing the commissioning of”. R3.4: Change the requirement to read: “Document identified vulnerabilities. Establish planned or completed dates relating to the mitigation or remediation of identified vulnerabilities.” Rationale: As worded, the language increases the compliance-tracking burden to all sorts of other documentation including action plans, plan status, etc. The proposed language shifts the focus of the requirement back towards a cyber security related outcome, i.e. mitigated vulnerabilities. This is accomplished by staying away from language that requires documentation overhead. Language on action plans should be moved into the guidance documentation.
No
No
R1.2: What is meant by transmittal, distribution and disposal requires further clarification and parameters in the Measures section. Suggested change: One or more documented and implemented procedures for handling BES Cyber System Information. Information handling procedures shall detail access, sharing, copying, transmittal, distribution, and disposal or destruction of BES Cyber System Information. R1.3: Suggested Change: Once each calendar year or a period not to exceed 15 months, assess adherence to its BES Cyber System Information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment. R2.1: Suggested change: Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except in other high impact or medium impact BES Cyber Systems, Associated Physical Access Control Systems, Associated Electronic Access Control or Monitoring Systems, or Associated Protected Cyber Asset), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information, the responsible entity shall maintain documentation that identifies who has possession of the device while it is outside of a Physical Security Perimeter. R2.2: Suggested change: Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, 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. If an applicable Cyber Asset is removed from the Physical Security Perimeter prior to action taken to prevent the unauthorized retrieval of BES Cyber System Information or destroying the data storage media, the responsible entity shall maintain documentation that identifies who has possession of the device while it is outside of a Physical Security Perimeter.
Individual
Richard Vine
California Independent System Operator

Yes
Yes
Yes
None
No
No
Yes
CIP-009-5 R1 – Suggest in Part 1.3 change the word “recover” to “restore”. In Part 1.4 change the word “recovery” to “restoration”. Define the terms recover, recovery, restore and restoration. Recovery – Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster. Restoration – Implementing actions for the repair or relocation of the primary site and its contents, and for the resumption of normal operations at the primary site. Part 1.4 reference backup media however this technology is antiquated and entities are using redundancy for restoration in which these requirements do not pertain. Change 1.3, 1.4, 2.1 and 2.2 to remove High Impact BES cyber systems from scope CIP-009-5 R2 - Part 2.2 references backup media however this technology is antiquated and entities are using redundancy for restoration in which these requirements do not pertain. Part 2.3 should reference EOP-008 in that EOP-008 would suffice meeting this requirement. Change 2.3 to say: “At least every 90 days, demonstrate that primary and backup BES cyber systems are independently capable of providing operational functionality to the associated control center.” Note: this wording attempts to be consistent with EOP-008 R6.
No
No
No
CIP-010-1 R1 - Part 1.4.1 – this can introduce double jeopardy in that non compliance with this requirements means non-compliance with the requirements in the referenced standards. Part 1.5.1 – remove the parenthesis but keep the text. What does “technically feasible” pertain to in this requirement? Part 1.5.2 – ISO/RTOs believe that testing in a production environment is not a sound security practice. CIP-010-1 R2 - Part 2.1 – Remove the words “continuously” CIP-010-1 R3 - Part 3.1 the requirement is redundant to 1.3. A vulnerability assessment should not be a compliance check. Part 3.3 and Part 3.4 define what is meant for a vulnerability assessment. Is it a “nessus scan” or is it a compliance check for CIP requirements? Applicable BES Cyber Systems and associated Cyber Assets differs between Part 3.3 and Part 3.4.
Yes
No
CIP-011-1 R2 - Part 2.1 appears to be two requirements and should be broken out if that is the intent. The current wording appears to pertain to cyber assets that contains BES Cyber System Information (i.e network diagram). The second sentence appears to pertain to Cyber Assets within an ESP.
Group
Hydro One
Sasa Maljukan
No
No
No
Request clarification on the EOP-004-2 reference in the R1 Rational. The previous version of EOP-004-2 was not accepted by the industry. What is the plan if future versions of EOP-004-2 are not accepted? Recommend changing the first bullet in R2 Part 2.1 from “By responding to an actual Reportable Cyber Security Incident; ” to “By responding to a Cyber Security Incident” since this covers the Reportable Incidents plus the non-reportable incidents Recommend updating R2 Part 2.3 since the existing language does specify a retention period. Recommend changing R3 Part 3.1 from “Review and update” to “Review and update, as needed,” since some years the Cyber Security

Incident response plan will not need updating Recommend changing R3 Part 3.3 from “Update the Cyber Security Incident response plan ” to “Update, as needed, the Cyber Security Incident response plan”
No
No
No
Is a Business Continuity Plan, where operations are transferred from the main control centre and continued at a back-up control centre, considered a recovery plan?
Recommend removing R1 Part 1.5 since this Requirement is forensics and/or Lessons Learned. The priority is Reliability or recovery, forensics. The title of this Standard is Recovery Plans for BES Cyber Systems. Request clarification on R2 Part 2.2. Is this a media test? Can the test be on a sample BES Cyber System? Recommend updating the Measure for R2 Part 2.3 to reference an updated Implementation Plan’s Initial Performance of Certain Period Requirements. This Requirement – Part combination is not identified in the existing Periodic Requirements. As requested in the first posting, request removing these bookends from this Measure Recommend changing from the reference from “R1.2” to “Part 1.2” in R3 Part 3.4 for correctness
No
No
No
Request clarification of R1 Part 1.1.2. Does “applications” mean “SCADA, EMS, State Estimator, IDC, etc” instead of “device drivers, DLL, applications included in an operating system or package, etc?” Request clarification of R1 Part 1.1.3. Would a version control tool/system (like CVS) demonstrate the custom software’s version? Request clarification on R1 Part 1.3. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005 and CIP-007? In R1 Part 1.3, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend removing the 30 day time frame in R1 Part 1.3 that applies to CIP-005 and/or CIP-007. Those Standards should specify their time frames. Recommend that the 30 days apply to only updating the baseline configuration (this Part) Request clarification on R1 Part 1.4.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R1 Part 1.4.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend removing R1 Part 1.4.2 because “availability” has not been part of the Requirements in the past, is not a FERC requirement and can be interpreted multiple ways In R1 Part 1.5, recommend changing from “Where technically feasible, for each change that deviates from the existing baseline configuration ” to “Testing cyber security control, where technically feasible, for each change that deviates from the existing baseline configuration” for clarity For R2 Part 2.1, recommend the previous version 5 words since this updated Part is not understandable Request clarification on R3 Part 3.1. We understand that each NERC Standard stands on its own. Please explain why CIP-010 depends on controls in CIP-005, CIP-006 and CIP-007? In R3 Part 3.1, recommend replacing the general references to CIP-005, CIP-006, and CIP-007 with the identified specific controls so there is no need for interpretations Recommend that R3 Part 3.1start with its purpose – for example, Active vulnerability assessment Request clarification on R3 Part 3.2. If this is a paper exercise it should be performed once every 36 months. Recommend that R3 Part 3.2 start with its purpose – for example, “Perform active vulnerability assessment, where technically feasibly….”. Recommend that R3 Part 3.3 start with “Perform an active vulnerability assessment, of the new cyber assets prior to business deployment, except for CIP Exceptional Circumstances and like replacements (same type of Cyber Asset with a baseline configuration that models an existing baseline configuration of the previous or other existing BES Cyber Asset).” Recommend updating CIP-010 R1’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R1 as “low” Recommend updating CIP-010 R2’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures shows R2 as “low”
Yes
No
Recommend moving the second paragraphs of R2 Parts 2.1 and 2.2 into a new Part 2.3 for clarity.