Name (63 Responses)
Organization (63 Responses)
Group Name (40 Responses)
Lead Contact (40 Responses)
Question 1 (92 Responses)
Question 2 (92 Responses)
Question 3 (92 Responses)
Question 4 (92 Responses)
Question 5 (91 Responses)
Question 6 (91 Responses)
Question 7 (92 Responses)
Question 8 (0 Responses)
Question 8 Comments (103 Responses)
Question 9 (0 Responses)
Question 9 Comments (103 Responses)
Question 10 (91 Responses)
Question 1 (90 Responses)
Question 12 (0 Responses)
Question 12 Comments (103 Responses)
Question 13 (0 Responses)
Question 13 Comments (103 Responses)
Question 14 (91 Responses)
Question 12 (90 Responses)
Question 12 (91 Responses)
Question 12 (0 Responses)
Question 17 Comments (103 Responses)
Question 12 (93 Responses)
Question 12 (93 Responses)
Question 12 (92 Responses)
Question 12 (92 Responses)
Question 12 (92 Responses)
Question 23 (0 Responses)
Question 23 Comments (103 Responses)
Question 12 (0 Responses)
Question 24 Comments (103 Responses)

Individual
David Proebstel
Clallam County PUD No.1
Yes
Yes
Yes
Yes
Yes
Yes
Yes
no comment
no comment
Yes
Yes
no comment
no comment
Yes

Yes
Yes
no comment
Yes
Yes
Yes
Yes
Yes
no comment
no comment
Group
Northeast Power Coordinating Council
Guy Zito
No
No
Yes
No
Yes
Yes
No
Recommend removing ", but not limited to," from R1 Part 1.1 Measure since the Measures are only guidance. Recommend removing "potential" from R2 Part 2.7 since an incident is determined to be real or potential during the follow up investigation. Request additional clarification on R2 Part 2.10 in the Application Guidelines. From the CIP-004-5 Table R2 - Cyber Security Training Program, the use of the terms interconnectivity and interoperability with regard to FERC Order No. 706 needs to be clarified to make the differences and applications of the terms understood. Request clarification on R4 Part 4.2 since it is not clear if the numbers should be read as "and" plus does the six months apply to all of the numbers? Prior versions of R4 Part 4.3 had exclusions for laws or collective bargaining agreements. Please add the exclusions or explain why the exclusions were dropped. Recommend different VSL thresholds for R3. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations. Recommend different VSL thresholds for R5. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations.
Request a more clearly worded R6 Part 6.4. The intent appears to be authorizing (electronic/physical) access to BES Cyber Systems Information. Request additional clarification in this Requirement and Application Guidelines. Note that Requirement 6.1.3 also uses "physical and electronic locations." In R7 Part 7.4, recommend changing "Requirements R7.1 and R7.3" to "Requirement R7 Parts 7.1 and 7.3." In the corresponding Measure, recommend changing "removal" to "revoke" for consistency with the Requirement. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. Recommend updating the R7's Violation Risk Factor in the Table of Compliance Elements. That VRF is "medium" while the Requirements and Measures show R7 as "low".
No
No
Recommend removing ", but is not limited to, " from R1 Part 1.1 since the Measure's scope already includes all of the possible Cyber Assets Measures should not dictate Requirements. If correct, then how can CIP- 005 R1 Part 1.5's Measure specify "intrusion detection system" when the Requirement does not specify a technology? Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from "intrusion detection system" to "detection system". Request for clarification on how the math for R1 is done in the VRF/VSLs.
Request clarification on R2 Part 2.1 – can the Intermediate Device be on the ESP? Can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from "Factors must be at

least two of the three following categories" to "Multi-factor include, but are not limited to" which allows future technology without a Standards update.
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are tested every 36 months.
Yes
No
No
No
No
For R2, request clarification if the SDT's intent is that the following timeline will be compliant or not. 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from "(1) immediate detection" to "(1) real time detection" to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect "deny by default" firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? The wording in the Measures column does not reflect what the Requirement is stipulating. Recommend removing "malicious" from R4 Part 4.1.4 since "malicious" is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious. For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe. Recommend that the number of assets should be another differentiator for R3's Low – Moderate – High – Severe. Recommend that the difference between R4's Low – Medium – High – Severe should be number of assets with two weeks throughout. Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low – Medium – High - Severe.
Request clarification of R5 Part 5.7. Does the technical feasibility apply to both "the number of unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful log in attempts" or only the "authentication attempts?"
Group
PPL Corporation NERC Registered Affiliates
Stephen Berger
Yes
No
Yes
No
Yes
No
Yes
1.) CIP-004 R2. Members of the SDT explained that the intent of "personnel who have …access…" be limited to company personnel, not vendors or others. This needs to be clarified if that is the intent.
1.) PPL Affiliates support the associated EEI comments for R6.3 : EEI Comments: Propose changing "The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP

Exceptional Circumstances." To "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances." In order to scope this requirement to the PSP.
No
No
1.) The definition of "External Routable Connectivity" is currently limited to a BES Cyber System that is accessible from a Cyber Asset that is outside its associated ESP. This should be expanded to include any Cyber Asset, not just BES Cyber Systems.
No
No
Yes
1.) R1: PPL Affiliates request removal of the "External Dial-up Connectivity" in the VSL table under the Severe VSL Column heading on the bottom right of page 23 of 29 in CIP-006-5. Dial-up connectivity is not included in the applicable columns associated with any of the CIP-006-5 Requirement Parts. 2.) PPL Affiliates have concerns about R1.4 and R1.6 and the 99.9% uptime requirement: PPL Affiliates appreciates all the value-added work the SDT has provided on the CIP Version 5 project. PPL Affiliates would like the SDT to consider changing R1.4 and R1.6 language to 'Implement controls that monitor access to the Physical Security Perimeter 24 hours a day, seven days a week.' PPL Affiliates believe that the requirement of having 24x7 controls restricts access appropriately. PPL Affiliates understand the requirement of 24x7 means very high availability. PPL Affiliates assumes the added language was intended to prevent frequent downtime causing risk to the control. However, the proposed phrase '(with 99.9% availability), for unauthorized circumvention of a physical access control into a PSP' increases documentation requirements without increasing BES reliability or reducing risk of unauthorized access. 3.) R2.1: PPL Affiliates request that the SDT revise R2.1 to read 'Require continuous escorted access of all Visitors within each PSP, except during CIP Exceptional Circumstances', with Visitors defined as 'Any individual (employee or non-employee) without unescorted physical access. PPL Affiliates' concern over the proposed language is that the phrase 'who are known or guests ' could be confusing. Additionally, defining visitor that is in other requirements proposed language clarifies those standards as well.
No
Yes
Yes
Yes
Yes
1.) R1.2: Regarding the requirement to "[p]rotect against the use of unnecessary physical input/output ports…", this may go further than the intent of the referenced FERC order from 3/18/2010, and in any case will be very difficult to implement as written. Prior discussions over the past couple of years had focused around the protection of unused network access ports. This has been broadened to every conceivable input/output port on an asset. Signage does very little to protect against this use, and other controls (like physically disabling USB ports to prevent connection of portable media devices) can limit recovery options during emergencies. The same is true with software solutions, though these can overridden by administrators. In general, PPL Affiliates support focusing on unused network ports and eliminate the rest. There are other protective controls in the requirements to deal with potential malware infections that could be introduced via portable media.
Group
CIP Version 5 Comment SME list
Gerald Freese
Yes
No
No

No
Yes
No
No
1. R2.1: While this requirement has been improved to clarify the entity is the one who identifies each role and the training required for each role, it is still not explicit that the training required are the topics in R2.2 through R2.10. 2. It should be made clear that R2.2 through R2.10 are a “pick list” to choose from for each role, and an entity has license to choose as few as one topic (or as many as 9 topics) for a particular role. 3. AEP is uncertain whether a single role, with all training (R2.2 through R2.10) is acceptable. For large entities, who don’t necessarily classify personnel by “role”, an extensive effort to create “roles” to offer narrowly differentiated instruction may not be commensurate with the reliability and security gain. Moreover, to fully utilize the “roles” at large entities (where personnel might “wear several hats”) may require hundreds of roles, with a single person filling multiple roles at the same time. This would result in a multidimensional matrix to determine training requirements, again not be commensurate with the reliability and security gain. AEP recommends that if it is acceptable to offer a single training program to multiple roles, the drafting team clarify that in the standards. 4.2.2, 4.2.3 - Is “six months” contiguous? If you go home to a residence in a different county / state on weekends, does that count against your six month boundary? Does it reset the timer? Or is the six months an absolute timer over the course of a year? Or some other interval? For large entities, this still represents an enormous amount of work by skilled functionaries who can figure out in which county a particular school is located, or where a particular work location is. Bottom line – it would be easy to hide a location where a crime occurred, and it would be impossible for the entity to figure out whether the list was truthful and complete. AEP believes this simply cannot be accomplished through the NERC regulatory model. Criminal background check vendors do not provide services that can verify the accuracy or inclusivness of locations where people have worked or attended school
4. R7.2: Similar to R7.1, problematic. Removing access by the end of the next calendar day Effective dates for new jobs could be Saturdays. This one also entails extensions of access for training, transition, etc. Reword. 5. R7.1 – AEP believes this should clarify that “complete the revocation” refers exclusively to “unescorted physical access and Interactive Remote Access.” Recommend adding the specific actions required in the wording of the requirement. 6. AEP believes that “voluntary” terminations (retirements, co-op students returning to school, etc.) really should be treated differently than “involuntary” termination actions. AEP suggests allowing for a difference between a mutually accepted “termination or separation” and a “termination for cause” and incorporating that concept into 7.1 and 7.2. 7. Since there is no requirement for revocation of “balance of access” R7.4 for Medium Impact BES Cyber Systems, is there a particular timeline required? Recommend a timeline be developed that provides auditable records for removing balance of access.
No
Yes
R1:) The applicability column should be modified to High and Medium with External Routable Connectivity. Standalone networks would be required to declare an ESP but there would be no requirements applied to the ESP. The ESP documentation of standalone networks would provide no reliability benefit to the BES. 2. R1.3: Need additional clarification on the requirement; perhaps through guidance. “Require inbound and outbound access permissions.” This requirement implies that in addition to establishing inbound Access Control Lists (ACLs) that a second set of ACLs is required for outbound communications. This is particularly a concern because it applies to Medium impact as well as High Impact Electronic Access Points. 3. R1.4: This requirement refers repeatedly to “dial-up connectivity.” Is dial-up connectivity defined to include for example, ISDN connections or is it limited to modems? Recommend that a definition be developed for “dial-up connectivity to eliminate confusion on the scope of the requirement. 4. R1.5: This requirement states that entities must “have a method for detecting malicious communications.” Malicious communications is a vague term that could apply to a host of items, not all of which would be associated with attacks on systems or networks. Suggest rewording to reflect the intent of the requirement. For example, qualify the term with a caveat such as “known or suspected to disrupt, destroy or otherwise compromise Electronic Access Points.”
R2: The applicability column for R2.1, R2.2, and R2.3 should be modified to High and Medium with

External Routable Connectivity or dial-up connectivity. Unless External Routable Connectivity or dial-up connectivity exists, Interactive Remote Access or an Intermediate Device does not exist.
No
Yes
Yes
1. R1.4 should be considered for removal. Monitoring 24x7x365 with a 99.9% uptime would require extensive resources and may be technically unrealistic. Recommend changing the actual requirement for 99.9% uptime to “document any disruption of uptime, root cause and remediation actions”, or words to that effect. 2. R1.3 – Asks for two or more different physical access controls to collectively allow physical access into Physical Security Perimeters. Would these be applied to the Physical Security Perimeter specifically or in a defense in depth concept, be applied to external fencing around the facility as well? Recommend that guidance be provided that clarifies how “defense in depth” should be viewed for the completion of this requirement. 3. 1.7 – The time frame of 15 minutes is questionable. Also, the administrative burden providing documented proof of initiation of alarm investigation is excessive and adds little if anything to increasing or maintaining BES reliability. The 15 minute time frame would mean that a 16 minute response time would be a violation. If we are keeping the documentation requirement, then the time limit needs to be extended. Recommend, however, that we remove the documentation requirements.
Yes
Yes
No
No
Yes
1. R2.3- Recommend a rewording of "vulnerabilities exposed by each security patch" to some thing closer to "vulnerabilities remediated by each security patch." The security patch is not what exposes the vulnerability. 2. R3.1- Is "or" appropriate in "deter, detect, or prevent malicious code"? This seems to indicate that an entity only has to "deter" malicious code, which could simply be addressed by a security awareness campaign. 3. R4.1- Recommend that this requirement be rewritten with a "where technically feasible" addition. 4. R4.1.4- Recommend that guidance provide a more concrete explanation of what would be included in "malicious activity."
5. R5.6- Recommend that the second measure be modified to include a dated attestation that passwords were changed. Lacking that, there is no consistent means of verifying that the requirement has been met.
Individual
Michael Falvo
Independent Electricity System Operator
No
No
No
Yes
Yes
No
No
For CIP-004-5, R2, IESO disagrees with the “role-based cyber security training” approach, and suggest SDT change this requirement based on or tailored to job function based training approach. In its current form, the “role-based” statement in this requirement infers that the training should be provided based on permissions or access should be role based. For CIP-004-5, R2.1, change “identification of each role” to “identification of roles based on job functions” required for BES cyber access. For CIP-004-5, R2.10, IESO suggests that SDT to modify this requirement to clearly to emphasise the intent of the requirement, as the current form does not give us a clear picture of what was intended. For CIP-004-5, R3, similar to the comments and rationale provided on CIP-004-5, R2, that the “role-based cyber security training” need to be replaced with training based on or tailored to job function.

For CIP-004-5 R6 Part 6.6, IESO suggests the removal of measure 2.A: “summary description of privileges associated with each group or role”. For CIP-004 R6 – Part 6.1 – 6.1.3: states “access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” This statement implies that having physical access to BES systems alone is enough for someone to gain access to the information residing within it, which is misleading. The building maintenance staff, such as Janitors, and many IT staff may have access to the data center where the BES system is situated; however, this does not grant them automatic electronic access to the system or the data residing within that system. For CIP-004-5, R7.2: IESO suggest that the one day duration to revoke access for reassignments or transfers is too restrictive and should be changed to a 30 day duration to complete these revocations. The sections CIP-004-5, R7.4, and 7.5 deal with termination, which is more risky scenario than reassignments and transfer actions, and prescribes a 30 day window to revoke access and IESO suggests the duration should be adopted for the rules outlined in CIP-004-5, R7.2 for reassignments or transfers.
No
Yes
For CIP-005-5, R1.5: IESO believes it is not appropriate to prescribe Intrusion Detection System (IDS) as the only measure for detecting malicious communication. In fact, IESO believes that it is reasonable to state that statements within a standard should only focus on requirements relating to a specific topic, and no specific technologies should be referenced anywhere within it as means to gain compliance.
No
No
No
For CIP-006 R1 – Parts 1.4 and 1.6: These rules require multiple controls must be in place for the monitoring, which IESO disagrees. We suggest SDT to change the phrase “Have Controls” to “Have Control(s)”. For CIP-006 R1 – Parts 1.5 and 1.7: IESO suggest the removal of the “BES Cyber Security Incident Response Plan”, since physical security incidents are not considered cyber security incidents.
No
Yes
No
No
No
For CIP-007-5 R3 - Part 3.1: IESO suggest the removal of the word “deter” from the requirement as it is not possible to “deter” malicious code from entering through an electronic communication. For CIP-007-5 R3 - Part 3.2: The second and third bullets reference technologies, which is not appropriate and should be removed from this section. This first bullet point alone is enough to measure the compliance of this requirement. For CIP-007-5 R4 and R3: For maintaining consistency throughout the standard, IESO suggest the use of “malicious code” rather than “malicious software”, which is referenced here. For CIP-007-5 R4.1.4: Unless the SDT defines what “malicious activity” is, the IESO suggests the removal of this phrase. For CIP-007-5 R4.2: The term “real-time alerts” is not defined, and using this term in the standard without the definition it is open for interpretation. With this current form, it is not clear whether “real-time alerts” are alerts triggered as they received by the monitoring facility or it is at the time of actually occurred on the target BES system. For CIP-007-5 R4.5: IESO believes the measure should include the clause “where automated processes and alerting are not possible” as part of the measure. It should not be necessary to maintain manual tracking and review of alerts, if alerts are triggered automatically and followed up through a ticketing system, for example.
For CIP-007-5, Part 5.1: The meaning of the term “user access” is not clear and needs to be defined. For CIP-007-5, Part 5.3: IESO suggests that the measure should be reworded to include “authorized access”: “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” For CIP-007-5, Part 5.4: IESO suggest the words “devices” and “instances of application” should be removed from the requirements to leave only “Cyber Asset”. The following is the suggested new requirement: “Change default passwords.

where technically feasible, unless the default password is unique to the Cyber Asset." For CIP-007-5, Part 5.5 and Part 5.6: Since IESO is a unionized work place, it may be difficult to obtain attestations from union members in order to satisfy second bullet within the measure for this requirement. IESO suggests adding a new measure that includes procedural control and a training aspect to handle this requirement. For CIP-007-5, Part 5.5.1: IESO request that this requirement should be reworded to remove the phrase "the lesser of" to the following: "Password length that is, at least, eight characters or the maximum length supported by the Cyber Asset", and Part 5.5.2 reword to "Minimum password complexity that is at least three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset." For CIP-007-5, Part 5.7: IESO recommends that the SDT to define the number of unauthenticated logon attempts and a threshold number that is reached before an alert is triggered. Without having these numbers defined within the standard requirements, it will be inconsistent between entities.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Yes
No
No
Yes
No
No
No
(1) Requirements R2, R3, R4, and R5 should be applicable to Medium Impact BES Cyber Systems irrespective of any External Routable Connectivity or dial-up connectivity. BES Cyber Systems and their component Cyber Assets generally have security controls and inherent vulnerabilities to insider threats whether or not they also have connectivity beyond the fence. (2) Part 2.10 properly requires training content on risks associated with a BES Cyber System's electronic interconnectivity and interoperability. This connectivity does not have to be beyond the Local Area Network, further supporting the need to make R2 applicable to all Medium Impact BES Cyber Systems. (3) The suggested evidence for Part 3.1 should be clarified to expect both the individual training records and the date access was first authorized. Both elements are necessary to demonstrate compliance. (4) R5.2 needs to be modified to require the personnel risk assessment to be updated prior to the seventh anniversary of the previous assessment. The use of the term "calendar years" could be misconstrued by the Responsible Entity as any time in the calendar year (January 1 – December 31) in which the PRA reaches its seventh anniversary, even though the requirement also states the expectation that the current PRA is no older than seven years. (5) The High VSL for R1 should be modified to require the missed awareness training to occur within the following calendar quarter. A failure to provide awareness training for two or more consecutive quarters should be a severe VSL. (6) The Moderate VSL for R2 should apply if the Responsible Entity failed to include 2 "or 3" of the required training content. (7) The guideline for R3 refers to CIP Exceptional Circumstances that are "approved" by the senior manager or delegate. CIP-003-5 / R1.10 only requires the Responsible Entity to document and implement provisions for declaring and responding to CIP Exceptional Circumstances. R1.10 does not prescribe a governance structure that requires senior manager or delegate approval.
(1) Requirements R2, R3, R4, and R5 should be applicable to Medium Impact BES Cyber Systems irrespective of any External Routable Connectivity or dial-up connectivity. BES Cyber Systems and their component Cyber Assets generally have inherent vulnerabilities to insider threats whether or not they also have connectivity beyond the fence. (2) The "and" at the end of Part 6.1.2 should be "and/or". (3) The evidence supporting Part 6.6 needs to demonstrate that user accounts have been properly provisioned, essentially access has been granted on the correct Cyber Assets with the correct access rights. (4) R7 should include provisions for documenting a transition period to allow for continued access for a defined period of time following a transfer. The time period for revoking unneeded access would commence with the expiration of the transition period. (5) Part 7.1 should include the requirement to disable or revoke all individualized domain user accounts held by the terminated staff. (6) The change rationale for Part 7.2 refers to a NIST SP 800-53 control requiring a

review of access. This could cause some Responsible Entity confusion as the requirement is to “revoke” access, not “review” such access. If the expectation is to revoke only the access the Responsible Entity has reviewed and determined to no longer be necessary, the requirement should be restated to reflect that expectation. (7) Part 7.4 should also include Medium Impact BES Cyber Systems or another requirement should be defined that includes the Medium Impact systems. As written, the Medium Impact BES Cyber Systems essentially fall through the cracks and individual user accounts will never have to be revoked. (8) Passwords for administratively privileged shared accounts should be changed much faster than the 30 calendar days specified in Part 7.5. (9) The second bullet of the example evidence for Part 7.5 should be clarified that password reset is only required if the individual being transferred no longer needs such access in the new position or role. (10) The guidance for R7.1 should also include the revocation of domain account access.
No
Yes
(1) Part 1.1 should also apply to associated Protected Cyber Assets as stipulated in the language of the requirement. (2) The measures for Part 1.2 still need a process to verify all Electronic Access Points have been identified. A network diagram does not demonstrate compliance by itself. (3) The percentages found in the VSLs will be difficult to determine. Does the percentage refer to “permit statements?” The number of Cyber Assets associated with the permitted access? The number of ports used permitted traffic? Something else? The VSL as written is too vague to be measurable. (4) The guidance for R1 discusses the limitations on the ability of a BES Cyber System to communicate through the EAP. This commentary appears to conflict with the requirement for an intermediate system (jump host) that essentially denies the ability of the Cyber Asset within the ESP to communicate with any other system outside of the ESP.
(1) R2 should also apply to Physical Access Control Systems and systems serving as Electronic Security Perimeter Access Points.
No
Yes
No
(1) The requirements need to be applicable to the associate physical access control and electronic access control and monitoring systems. (2) The term “availability” as used in Part 1.4 and Part 1.6 needs to be defined. Does the availability calculation include outages for planned maintenance activities, or only unplanned outages? (3) The testing required by Part 3.1 needs to include the logging and monitoring systems to verify proper operation. (4) The Moderate and High VSLs for R1 need additional clarification. The difference between unauthorized physical access and unauthorized circumvention of a physical access control is not clear. The expectation needs to be explained. (5) The Lower VSL for R3 needs to refer to 12 “calendar” months of outages to comport with the language of the requirement. (6) The description of Alarm Systems used to monitor physical access in the guidelines for R1 states the alarm needs to provide for “immediate” notification. The requirement in Part 1.5 states the notification must occur within 15 minutes of detection. (7) The description of Video Recording used to log physical access needs to clarify that the recorded video needs to be date/time stamped. (8) The guidelines for R1 needs to define the difference between unauthorized physical access and unauthorized circumvention of a physical access control. (9) It is not clear from the FERC comments in Order 706 that two complementary controls can be implemented on a single Physical Access Control System as stated in the guidelines for R1. Paragraph 562 (the FERC NOPR “proposal”) states that “use of a minimum of two different security procedures would, for example, enable continuous security protection when one of the security protection measures is undergoing maintenance and provides redundant security protection in the event that one of the measures is breached.” Implementing two controls on a single access control system does not address the single point of failure concern. (10) The guideline for R1 requires physical barriers for any opening exceeding 96 square inches with one side exceeding 6 inches. This explanation needs to be modified to stipulate the side exceeding six inches is the short side. Otherwise, this explanation could result in nonsensical dimensions requiring physical barriers. (11) The drafting team should consider the use of electronic barriers (e.g., infrared beams) in lieu of physical barriers for openings exceeding 96 square inches. There may be operational or technical limitations that preclude the use of physical barriers, such as impeding air flow through the protected opening. (12) The guidelines for R2 need to clarify that general logging of entry into a facility that is not entirely a PSP does not constitute logging of

entry into the PSP. The guidelines also need to address logging requirements when entering multiple PSPs in the course of the visit (either moving from one PSP to another or entering progressive perimeters). (13) The equipment to be tested per the guidelines for R3 should include the logging and monitoring systems (e.g., door contacts that generate forced open and door held alarms).
No
No
No
No
No
(1) Part 1.1 needs to consider more than “listening” ports. An unexpected connected port could indicate a successful compromise of the Cyber Asset with the malware making an outbound connection to a Command and Control system. (2) The “signage” referenced in the example measures for Part 1.2 is a weak control that does not provide an adequate level of protection as required. (3) Security patch management is a key fundamental control that should be applied to all Cyber Assets, including Low Impacting BES Cyber Systems. (4) Allowing the Responsible Entity to select a SCADA vendor as their source of potentially applicable patches increases the risk to the BES. The Responsible Entity needs to monitor the original source of a patch, such as Microsoft for Windows patches, and assess applicability within 30 calendar days of the initial patch release. There is a difference between “applicable” and “installable.” Waiting for the SCADA vendor to “certify” a patch as compatible is an issue of ability to install, not applicability. Requiring the Responsible Entity to assess for applicability based on the original patch provider’s release does not jeopardize any contracts or maintenance agreements. The entity still has the ability to self-determine the patch can or cannot be installed or wait for the vendor certification before installing. In the interim, the Responsible Entity, having determined a patch is applicable, can and should implement compensating measures until such time as the patch is certified. Allowing the Responsible Entity to rely upon a SCADA vendor’s certification as the trigger for the assessment process could result in patches that are not considered for an excessive period of time if the vendor does not report out the patch until it is “certified.” (5) Part 2.3 needs to be more specific as to the expectation of patch implementation. Part 2.3 only requires the entity to develop a timeframe to complete the identified mitigations, with no parameters defining an acceptable timeframe. For example, a Responsible Entity that chooses to not install any Oracle patches nor apply any interim compensating measures except as part of a planned end-of-life server upgrade would have to be found compliant, yet has done nothing to mitigate the risk imposed by the un-patched vulnerability. That renders Part 2.3 nonsensical. (6) Malicious code prevention is another fundamental control that should apply to all Cyber Assets capable of running anti-malware solutions, including Low Impacting BES Cyber Systems. (7) Updating anti-malware signature files every 35 days opens a window of unacceptable risk. As written, the requirement of Part 3.3 could possibly be gamed to not install any recent signature file. The Change Rationale expresses the desired outcome, but the requirement is not as clear. (8) Signature files still need to be “staged” (a form of testing) before implementing in the production environment. There is too much past history of a corrupted or faulty signature file being implemented that then improperly determines key software to be malware. This could be catastrophic if numerous Responsible Entities using the same anti-malware provider all implement a faulty update that quarantines or deletes critical software systems used to manage BES reliability. (9) The suggested evidence for Part 4.1 should include samples of logs demonstrating that the appropriate events are being logged. (10) Part 4.2 should prescribe a minimum expected set of security events for which alerts should be issued (if the Cyber Asset is capable of detecting and logging those types of events. Examples include failed login attempt threshold exceeded, account lockout, key software failures, and virus or malware alerts. (11) What is the expected delivery time for a “real-time” alert? (12) The example measures for Part 4.2 should include examples of issued alerts. (13) Part 4.3 presumes, but does not prescribe, a mechanism for monitoring for and detecting logging system failures. (14) Part 4.4 should also apply to Medium Impact BES Cyber Systems not in a control center that are capable of generating and storing security event logs. (15) Part 4.5 needs to define minimum expectations for sampling logged events. For example, is 1 out of 100 logs adequate? 30 minutes of logs in the two-week period? Ideally, an event log analysis tool (SIM, SEM, SIEM, or SEIM) should be required in the control center environment, especially for High Impacting BES Cyber Systems. (16) The guidelines for R1 need to discuss the importance of monitoring more than just Listening ports (see comment 1, above). (17) The guidelines for R2.1 need to discuss the difference between applicable and implementable (see comment 4, above). (18) The guidelines for

Part 2.2 state that the Responsible Entity must be allowed to evaluate their individual risk exposure and determine if any compensating steps are to be taken. This is, in effect, acceptance of risk. FERC has already clearly stated that Responsible Entities cannot accept risk in Order 706. (19) The guidelines for Part 2.2 should discuss what “applicable” means. It is not clear from the discussion that Responsible Entities are only required to monitor patches for installed software. (20) The guidelines for Part 3.3 should discuss the importance of staging (“testing”) anti-malware updates before implementing into production. (21) Alerts on a system display, as referenced in the guidelines for Part 4.2, only work if the display is monitored. The guideline needs to make that concept clear.
(1) System access control is a fundamental control that should also apply to Low Impacting BES Cyber Systems. (2) Part 5.2 needs to clarify what is meant by “generic account types,” Does this, for example, include the “IWAM” and “IUSR” accounts created with the installation of Microsoft IIS? (3) When should default passwords be changed per Part 5.4? (4) Allowing a default password to remain unchanged per Part 5.4 is a very poor control in light of the recent RuggedCom issue where the default password was unique to the device but was based on a readily available piece of information, the MAC address, and easily determined. This control only makes sense if the unique password is truly random, such as might be the case with the “IWAM” and “IUSR” user accounts associated with Microsoft IIS. (5) Part 5.5 should require password complexity and other settings to be technically enforced to the maximum extent possible. (6) Part 5.7 should define the minimum acceptable failed login attempt threshold parameters. (7) The High VSL for R5 refers to failing to implement procedures to authorize the “use of” certain account types. Requirement R5 does not require authorization of “use”, only enablement. (8) The Severe VSL for R5 includes criteria for failure to implement procedures for password-based user authentication. Does this inadvertently mandate the use of passwords? Does it require password procedures even if passwords are not used? (9) The guidelines for R5 need to define what a “generic” account is. (10) The guidelines for Part 5.5 states the technical or procedural enforcement of password parameters are only required where passwords are the “only” credential used to authenticate individuals. Requirement R5, Part 5.5, does not contain the same stipulation. (11) The table at the end of the R5 guidelines needs modification. The table should make it clear that shorter passwords need to be changed more frequently. Additionally, the suggested change periodicity of two years or more for system account passwords with 25+ pseudo-random characters is inconsistent with the stated requirement to change passwords at least annually.
Individual
Mario Lajoie
Hydro-Quebec TransEnergie
Yes
No
Yes
Yes
Yes
No
No
(1) We agree with the comments provided by the NPCC TFIST on CIP-004 (2)Change table in 2.1 "Identification of Each role" by "identification of ROLE
(1)E7.5 - Technical Feasibility Exception (TFE) should be allowed (2) the requirement (R7) should apply only on interactive account.
No
No
(1) We agree with the comments provided by the NPCC TFIST (2)E1.5 - We don't think that we need to deploy an IDS for every ESP. The requirements should requires that some IDS should be deployed between the ESP Access point and the Internet but with no particular specification. This way, we could deploy a few IDS within our corporate network at the most critical node instead of deploying and managing an IDS for every ESP. So we would like the requirements to let the entity decide where to strategically place IDS based n their own network structure and also, based on their own risk assessment and analysis. (3) We believe that the "intermediate device" should be protected by a PSP but should not be in the same EAP that BES CYBER ASSET.

(1) We agree with the comments provided by the NPCC TFIST
No
No
No
(1)We agree with the comments provided by the NPCC TFIST (2) Request for clarification on R1.5 and R1.7 have to do physical and human intervention within 15 minutes of detection. This is not possible for a remote site where there is no staff on site. (3) CIP-006-5 R2 The non-compliance during emergencies should not lead violations (4) We recommend changing the testing in R3 Part 3.1 so that the High Impact Bes Cyber System are tested every 24 months and Medium with external routable are test every 36 MONTHS.
No
No
No
No
Yes
(1) R1.2: Evidence may also include rationale for use of necessary and unprotected physical input/output ports. (2) R2.1: "a patch management program" should be specified directly in R2 instead of R2.1 as the latter should only cover the tracking requirement of this program a patch management process doesn't "include" a patch management program, although the opposite could be true. (3) R2.3: Replace "exposed" with "adressed", as patches don't expose vulnerabilities. (4) HQT believes that timeframes given for R2: Security Patch Management (30 days) to make plan and R3.3 Update Malicious Code Prevention (35 days) should not be applied to all Medium Impact BES Cyber Systems but only to Medium Impact BES Cyber Systems with External Routable Connectivity. (5) Timeframe should be longer for Medium Impact BES Cyber Systems without External Routable Connectivity. Rationale: (a) because they are less reachable, they are less prone to an attack, that doesn't mean no protection is required, but it's lesser urgent than those with External Routable Connectivity; (b) without External Routable Connectivity, there is no easy technical means to automatically update security patches or signature files at such relative high frequency and mostly require manual intervention and travelling. By letting as drafted, Utilities will avoid implementing code protections that use signatures or patterns in Medium Impact BES Cyber Systems without External Routable Connectivity that could help to enhance the protection of those Cyber Assets even if those protections are not using the most recent signatures or patterns file. (5) We support the TFIST NPCC comment about CIP-007 R4 (6) Bug WITH Rational of R4 : we are difficulty to compliant with "immediate detection" (7) R4.3 : We consider it to be not required. 24hr delay is too much short and too many operational and temporary stuation may arise which come back to normal shortly after (24-48hr). Because of the distances it would be impossible to make a correction procedure in some cases in next calendar day (8) We support TFIST NPCC comment about R4.5
Individual
Thomas A Foreman
Lower Colorado River Authority
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
R 1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages.
Yes
Yes
Yes
No
No
In R4.1, we recommend the addition of the term “Where technically feasible” for all of the sub-requirements.
In R5.2, change the wording as follows: The Responsible Entity must document enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). In M5.2, change the wording as follows: Evidence may include, but is not limited to, a listing of enabled default or generic account types in use. R5.3 - Remove the word “authorized” from this requirement. This could be interpreted as requiring an additional authorization for access to these shared or default accounts. R5.4 – Change wording to: Change default passwords where technically feasible.
Individual
Glen Sutton
ATCO Electric
Yes
Yes
Yes
Yes
Yes
Yes
No
R7.2 requires, for reassignments or transfers, unnecessary electronic and physical access is revoked by the end of the next business day. The time constraint seems to be excessive for internal moves. Consider increasing the time frame (i.e. 3 business days) for this requirement.
Yes
Yes
R1.1 does not list “Associated Protected Cyber Assets” in the applicability column but lists them in the requirements column. Associated Protected Cyber Assets should appear in the applicability column. CIP-005 no longer lists Associated Electronic and Monitoring Systems or Associated Physical Access Control systems for any of the CIP-005 perimeter requirements. It does not seem that this is a step forward in security for these systems. Question: Is it the intention of the SDT to not require perimeter security for Associated Electronic and Monitoring Systems or Associated Physical Access Control systems?
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Request for clarification: R4: It is unclear in R4.2 what is meant by “detected failure of 4.1 event logging”. Is this to be taken as event failures (unsuccessful login attempts) or failures of logging sources to correctly log events?
Individual
Ed Nagy
LCEC
Yes
No
Yes
No
No
Yes
No
Comment: 1) R7.2 Needs to state “interactive remote access” as in R7.1. Other electronic access such as user account and shared account requirements are covered in R7.4 & R7.5.
Yes
Yes
No
No
No
Comments: 1) 1.4 states that controls must be in place to monitor the physical security perimeter 24/7. Need to clarify what is meant by this. Does this mean monitoring of all access points or is there something more being implied? If the intent is to monitor the access points, this should be stated. 2) The requirement for 99.9% availability does not state a period which will lead to subjectivity and auditing issues. Is the intent for this to be a monthly or annual metric? 3) 1.5 no longer requires response to unauthorized access attempts but uses the term circumvention of a physical control. I think this is a positive change from a compliance perspective but leaves a gap that could be addressed through periodic PACS log review. 4)1.6 & 1.7 should be re-worded to focus on unauthorized access to the PSP containing the PACS as opposed to the PACS itself. Same comment on availability metric without period. 5) 1.8 Need to determine what is acceptable when it comes to identifying an individual. For example, is an access card and PACS log considered acceptable evidence? An auditor could interpret that a stronger level of authentication be required. Does including the individuals name on a sign in sheet constitute identification? 6) 1.9 Retention requirement of 90 days for logs will not match the audit period or expectation of auditors unless it is made clear that the solution and process be audited but that sampling can only be required within the retention period. Comments: 1) 2.1 The concept of continuous escorted access makes sense but should be more clearly defined. If the escort and visitor enter and exit the PSP at the same time, is this considered to be sufficient evidence of “continuous escorted access”? 2) 2.3 Retention requirement of 90 days for logs will not match the audit period or expectation of auditors unless it is made clear that the solution and process be audited but that sampling can only be required within the retention period Comments: Table R3 Many physical access control systems do not include any maintenance requirements so this should not be required. Testing needs to be more clearly defined. Is the expectation that each access control device be tested to ensure operation when presented with the appropriate credentials and that access is denied when presented with the incorrect credentials?
No
No

Yes
No
Yes
Comments: 1) R1.1 Should not include the term services as the clear intent with this requirement is to enable only the required logical network ports or sockets. If a service is network based, it is covered by the port/socket. Comments: R2 The patch management process should include a periodic review of all patch sources. (30 days is appropriate). The applicability review should take place within 30 days of the date the site/source review was executed. Using availability of the patch will be difficult to manage from a compliance and auditing perspective. For example, the monthly source review could take place on the first of the month; a patch is released on the second day of the month but is not identified until the first day of the next month. Is the patch release date available on the vendors site? Will it still be available at the time of the audit? Comments: R4.4 Retention of logs for 90 days makes sense but does not meet the expectation of auditors. The standards must differentiate between auditing of the systems and processes that are in place to meet the requirements and the retention of logs for the entire audit period. Auditors expect to be able to ask for logs for any day within the previous three years in most cases.
Group
NRG Energy Companies
Alan Johnson
Yes
No
Yes
No
Yes
No
No
In requirement R2, replace the reference to role-based training with training appropriate to job function. This will eliminate potential confusion about the term “role-based”, which is often associated with IT access control. Suggested wording “Each Responsible Entity shall have a cyber security training program, appropriate to job function, to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.”
In R7.2, replace “…that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.” with “…one calendar day after the determination that access is no longer needed.” Generally, there is no reason to believe a reassigned or transferred employee is a threat to security and there will be occasion where these employees will need temporary continuing access (e.g. training new employee in position). Please clarify what are user role categories in Requirement R6.6.
Yes
No
In Requirement 1.5, the Measure could be interpreted to prescribe the use of an Intrusion Detection System, however, such a system is not prescribed in a requirement. The references to IDS should be removed. Other systems and tools can be used to detect malicious communications.
1. The definition of Interactive Remote Access (or applicability of CIP-005-5 R2.1, R2.2 and R2.3) should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal/zero reliability benefit and significant cost associated with applying this requirement to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of Interactive Remote Access as follows: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic

Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications." This definition is also found on Comment Form D, question 12. 2. From V5R1 Consideration of Comments – Definition of EAP section (this helps justify that Interactive Remote Access should not apply to serially connected/non-routable/non-network connected devices): "The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs." 3. Suggest adding guidance to provide clarity on what is meant by a remote access client and/or remote access technology. In addition, how would two factor authentication be monitored for outside vendor support?
No
Yes
No
1. Requirements R1.4 and R1.6 call for 99.9% reliability of monitoring systems. The documentation required to prove this level of reliability would require extensive resources to satisfy. In addition, it's not clear if these requirements allow for alternate or redundant controls when the primary system is unavailable. For physical access controls, CIP standards should not be so restrictive as to limit options to only electronic methods. The 99.9% availability should be replaced with an allowance for documentation of system maintenance or outages with use of compensatory activities for monitoring. 2. In Requirements 1.5 and 1.7, an exception should be made for system maintenance or outages that last more than 15 minutes so they do not automatically create a violation. During a system maintenance activity such as required patching, the alerting system may not be functional for a period of more than 15 minutes. Unauthorized access may be detected, but not alerted during the maintenance activity. The performance of a required activity such as patching should not put a company in violation of the standard. Allow for documentation of system maintenance or outages and the use of compensatory measures, if required. 3. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection."
No
Yes
Yes
No
No
1. The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity." The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. 2. Modify Requirement R 4.1.3 from "detected and logged malicious software…" to "detected and logged malicious code…" 3. Eliminate requirement R4.1.4. The term "malicious activity" is ambiguous. 4. In Requirement R4.2, revise language to replace real-time with an actual target timeframe and refer to capability of the system rather than using the term technically feasible. Suggested language "Issue and alarm or alert, within 15 minutes, for security events that the Responsible Entity determines necessitate an alert, that includes, as a minimum, each of the following types of events where the BES Cyber System is capable:". Modify Requirement 4.2.1 to read "detected events per R4.1; and". 5. Requirement 4.3 is not consistent with 15 minute interval to address monitoring.
1. In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read "Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible". 2. Applicability for R5.2 should be the same as R5.3 – only applicable to external routable connectivity. Change "delegate" to "delegate(s)" as companies may choose to have one or

more delegates, depending on how they structure their program. Alternatively, consider removing R5.2 and R5.3 altogether as these requirements may already be covered by CIP-004 R6. 3. Requirement 5.5 –will this new requirement remove the CAN-017 requirements? 4. Requirement 5.6- this should consider account authorization not user accounts as explained in R5.1. 5. CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold.
Group
Duke Energy
Greg Rowland
Yes
No
No
No
Yes
No
No
(1) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Associated Electronic Access Control or Monitoring Systems”. The last statement, “Examples include, but not are limited to firewalls, authentication servers, and log monitoring and alerting systems” is not part of the defined term of Electronic Access Control or Monitoring Systems. Duke suggests removal of the last statement as an apparent prescriptive list of examples may not always be true. Firewalls may exist which don’t control access to the ESP(s) or BES Cyber Systems, so they shouldn’t fall into consideration of this applicability. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (2) Requirement R2.2. The requirement states “Training content on the cyber security policies protecting the Responsible Entity’s BES Cyber Systems”. This does not match the applicability section of the R2.2 as other types of systems are also included such as Associated Physical Access Control Systems. This makes it very confusing as to what the requirement is actually applicable to. Duke suggests not repeating any terms used in the applicability section within the language of the actual requirement and instead using a phrase such as “protecting the Responsible Entity’s applicable Cyber Assets as listed in the “Applicable BES Cyber Systems and associated Cyber Assets” section of R2.2”. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Requirement R3.1. Duke suggests that the phrase “and documentation” be removed from the requirement. This phrase is redundant to the requirement R2 which requires the documentation of the training needed. (4) Requirement R3.1 and R3.2. Duke is concerned with the lack of clarity as to who is to receive the training as required by R3.1 and R3.2. Currently, no language exists within the requirement as to who needs to receive this training and Duke does not feel that is acceptable. With the current wording, one could simply train a single individual before granting an entire group of people access to BES Cyber Systems. Duke does not believe that is the intent of these requirements and believes the standard should be specific as to who is required to receive the training. (5) Requirement R4.1. Duke is confused by the term “initial” in this requirement. What is the drafting team’s intent of this word? Is the intent that even those individuals who are covered under an existing PRA for the previous versions of CIP would be required to get another “initial” PRA prior to implementation of version 5? Duke feels that would be unnecessarily burdensome and costly. Duke is also concerned by the implications of demonstrating “initial” PRA’s for compliance. Would Duke be expected to retain evidence for individuals from audit to audit, to continue to prove that each individual had an “initial” PRA, even if it was conducted 10 years ago and a new 7-year has been conducted since? The wording of the requirement would seem to suggest this. (6) Requirement R4.2. Duke suggests modifying the last phrase of “the subject has, for six months or more” to “the subject has, for six consecutive months or more” to further clarify that the time duration only makes sense if it is assessed consecutively. (7) Requirement R4.2.1, R4.2.2 and R4.2.3. These statements need to be assessed as a list of “OR”s. The current wording suggests that only the locations that meet all 3 criteria need to be reviewed in the process. (8) Requirement R4.4. Duke suggests removing the requirement R4.4. Duke does not believe this statement should warrant its own requirement. As currently drafted, this would require an entity who has no contractors or service vendors with access to still have a process or criteria for verifying that the PRAs are performed in

accordance with R4.1 to R4.3.
(1) Rationale for R6. Duke suggests that the last statements in the rationale section be incorporated into the language of the actual requirements. The statements, “For BES Cyber Systems that do not have user accounts defined, the controls listed in Requirement R6 are not applicable. However, the Responsible Entity should document such configurations”. These statements are critical to meeting compliance with R6 and need to be incorporated into the language of the requirements as opposed to existing solely within the rationale section. (2) Requirement R6.1. Duke suggests that the phrase in this requirement be modified to read, “Designate one or more individual(s), by name or by role, to authorize:”. This will give entities the flexibility in designating a job role with the authority to make specific changes without having to change its documented designees every time there is a person entering or leaving a role. (3) Requirements R6.2, R6.3, and R6.4. Duke suggests that the phrase “Responsible Entity” within the requirement be replaced with “individual(s)”. This clarifies that the authority lies specifically within the individuals who have been delegated that function and that the Responsible Entity is not itself directly involved in the authorization process. (4) Requirement R6.4. Duke is concerned with the existing language of this requirement and that the physical locations where electronic BES Cyber System Information would also have to be restricted access areas. These locations, may be off-site, or may not be controlled by the entity. Duke suggests the splitting of R6.4 into two different requirements. The first requirement should require the entity to identify the repositories that store either physical media containing BES Cyber System Information (paper copies) or the electronic storage of BES Cyber System Information. The second requirement should be the authorization of access to only those designated repositories that have been identified by the entity. (5) Requirement R6.6. Duke would like to propose the following rewording of this requirement to “For electronic access, verify at least once each calendar year, not to exceed 15 calendar months, that the user accounts, user account groups, or user role categories on applicable Cyber Assets, and their specific, associated privileges are correct and are those the Responsible Entity determines necessary for performing work functions.” The existing wordings use of the word “all” could be misinterpreted that this requirement must be met for more devices than those listed in the applicability section of the requirement. (6) Requirement R7.2. Duke proposes the following rewording of this requirement to “For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the notification of reassignment or transfer.” The inserting of the phrase “notification of” emphasizes that the Responsible Entity can only act as fast as it receives appropriate internal notification of a change requiring the revocation of access. (7) Requirement R7.5. Duke proposes the following rewording of this requirement to “For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the notification of termination action, reassignment, or transfer of the user. If the Responsible Entity determines and documents that CIP Exceptional Circumstances require a longer time period, change the password(s) within 10 calendar days following the end of the CIP Exceptional Circumstances”. The inserting of the phrase “notification of” emphasizes that the Responsible Entity can only act as fast as it receives appropriate internal notification of a change requiring the need to change passwords. The replacement of the phrase “extenuating operating circumstances” with “CIP Exceptional Circumstances” is meant to use the specific defined term created for an event like this. (8) Application Guidelines Section for R7. Duke is concerned with the scenario of “death” appearing as a termination action that needs to follow the requirements in R7 for immediate initiation of access revocation. Duke recommends that the Guideline section clarify that the “effective date and time of the termination action” in the “death” scenario not to begin until the Responsible Entity is notified.
No
No
(1) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Medium Impact BES Cyber Systems at Control Centers”. The phrase “located at a Control Center” is not consistent with the application of CIP-002. CIP-002 requires the identification of BES Cyber Systems “associated” with a Control Center, not just those physically located at a Control Center. Duke suggests using the word “associated” here instead of “located at”. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (2) Background section, “Applicability Columns in Tables:” section. Duke is concerned with the description for the bulleted item, “Medium Impact BES Cyber Systems with External Routable Connectivity”. The last sentence states that “This also excludes Cyber Assets in the BES Cyber System that cannot be

directly accessed through External Routable Connectivity". This is confusing. CIP-002 allows for the grouping of Cyber Assets into Cyber Systems such that the applicability to the system can be analyzed to the whole and protections can be applied accordingly, as opposed to each individual Cyber Asset. Duke recommends that this theme be carried consistently throughout the each standard and once a Cyber System is grouped, it should not have to be broken up to assess individual Cyber Asset impact. In this circumstance, either the system itself has External Routable Connectivity or it doesn't, and protections can be applied to the system as a whole. NOTE that this comment applies to ALL CIP Standards CIP-002-5 through CIP-011-5. (3) Measure 1.1. This measure is inconsistent with the respective Requirement R1.1. Duke suggests striking the phrase "uniquely identifiable" as there is no requirement to uniquely identify each Cyber Asset within each ESP. This comment assumes that corrections are made such that the Requirement R1.1 is only applicable to the applicability section and not to the words currently stated within the requirement. (4) Requirement 1.5. The requirement here needs to be clarified as to where the entity needs to be able to detect malicious communications. It is Duke's understanding that the intent of this requirement is to detect malicious communications that originate outside the ESP and attempt to transverse the boundary of the ESP through one of the applicable types of Electronic Access Points. If this is true, then the requirement should be reworded to say, "Have a method for detecting malicious communications originating on a Cyber Asset outside of the Electronic Security Perimeter that attempts to transverse the boundary of the Electronic Security Perimeter through one of the applicable types of Electronic Access Points".
(1) Requirement R2. Duke recommends striking the phrase "where technically feasible" and inserting it at the end of every sub-requirement for R2. In previous versions, it is not very clear that statements within a main requirement effectively flow down to the sub-requirements. In addition, it is difficult to determine why creating a process would not be technically feasible as the current language suggests. (2) Requirement 2.1. Duke recommends rewording the requirement to "Utilize an Intermediate Device such that the authorized user initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset". Duke suggests replacing the term "Cyber Asset" with "authorized user" as it more closely aligns with the proposed definition of Interactive Remote Access as originating from a human and not from an automatic process that may be running on a Cyber Asset. (3) Requirement 2.2. Duke recommends striking the phrase, "in order to protect the confidentiality and integrity of each Interactive Remote Access session". This phrase is opinion as to what purpose encryption could serve and not integral to the requirement. Thus Duke recommends removing it. (4) Requirement R2.3. Duke recommends rephrasing the beginning portion of this requirement to read, "Require multi-factor authentication to the Intermediate Device for all Interactive Remote Access sessions". This wording change clarifies that multi-factor authentication is only needed at one point during the process and not to every element needed to support Interactive Remote Access.
No
No
Yes
(1) Requirements R1.2 and R1.3. The current wording of these requirements can be read to mean that ONLY those with individuals who have authorized physical access can enter a PSP. This would specifically exclude visitors from ever entering the PSP, even if allowed by another requirement. Duke suggests appending the requirements with the following language, "This requirement does not apply to visitors who may enter a Physical Security Perimeter in compliance with CIP-006-5 R2.". (2) Requirement R1.3. Duke recommends replacing the phrase "controls" with "authentication methods". This change allows entities the flexibility of utilizing two or more access authentication means that may exist with the same control. For example, a badge reader that has a keypad for a user to also enter a PIN number may be misinterpreted as a single control since it resides within the same device. This clarifies that this type of device is multiple authentication methods and therefore in compliance with the requirement. (3) Requirement R1.4. Duke is concerned with the current language of this requirement. The current wording suggests that the entire Physical Security Perimeter must be monitored for unauthorized access. This could incorrectly be interpreted to mean that the walls/ceiling/floor/etc. of the perimeter themselves must be monitored. The usage of the 99.9% availability term is also very confusing, as there is no guidance as to how this can be achieved or to what the availability is to be measuring (over what time period? to any one device? to the system as a whole? etc.). Duke recommends that this requirement be written more similarly to CIP-007-5 R4.3 where alerts need to be generated when monitoring tools are not available. Also enabling the use of

an alternative measure to support monitoring while the primary tool is unavailable will aid the entities in meeting availability concerns. (4) Requirement 1.5. Duke recommends replacing the term “circumvention” with “access”. Duke feels that the word access more adequately reflects the concern of being alerted to a situation only once actual access is obtained, not necessarily just when a control is circumvented (in the possible instance of circumvention without anyone actually gaining access to the restricted area). (5) Requirements 1.6 and 1.7. Duke recommends removing requirements R1.6 and R1.7. There is no requirement requiring Physical Access Control Systems to be within physically protected boundaries such as PSP’s, thus having controls to monitor and alert to unauthorized access are inconsistent with the remainder of CIP-006-5. (6) Requirement R1.8. Duke recommends removal of the parenthetical, “through automated means or by personnel who control entry”. This phrase is unnecessarily prescriptive and the requirement should allow the entities to log entry with whatever vehicle they determine is appropriate for their situation. (7) Requirement R2.1. Duke recommends rewording the parenthetical to “individuals who are not authorized for unescorted physical access). It is not necessary for the requirement to state that visitors have to be known or be guests. The requirement reads more clearly when visitors are acknowledged to be anyone who does not have authorized access.
No
No
No
No
No
(1) Requirement 2.2. Duke suggests that 30 days be changed to 35 days to allow for monthly patch cycles and increase efficiency. (2) Requirement R2.3. The change rationale section includes a lot of good and detailed explanation that may be better served within the actual requirement. Duke recommends that the wording be re-evaluated to determine if any of the language can be moved to the requirement to clarify the drafting team’s intent. (3) Requirement R2.4. Duke recommends striking this requirement. The need to implement the plan is redundant with the combination of the main requirement R2 requiring that entities implement the processes that are developed to meet the sub-requirements, in this case R2.3. The only difference here is the inclusion of “CIP Exceptional Circumstances” which should be moved to the language of R2. (4) Requirement R3.3. The requirement here to update “protections that uses signatures or patterns” incorrectly assumes a specific type of technology is being used to meet compliance with CIP-007 R3. If an entity does not employ a technology that uses signatures or patterns for malicious code prevention, that entity would still have to have a documented process to meet compliance with CIP-007 R3.3 (per language in the main requirement CIP-007 R3). (5) Requirement R3.3. Duke believes that the 35 calendar day update is too prescriptive and recommends a 95 calendar day update instead. Duke feels that this update period is better suited to the industry environment. (6) Requirement R4.1. Duke recommends rewording the first part of the requirement to read, “Log events for identification of, per device capability, each of the following types of events:”. This clarifies the drafting team’s intent that TFE’s are not required in this sub-requirement, if the device is not capable of detecting or logging the type of event found in the sub-sub-requirements. (7) Requirement R4.2.1. Duke recommends that the term “malicious activity” be replaced with “Cyber Security Incident”. Duke feels Cyber Security Incident better reflects the intent of the drafting team. If this is not the intent, Duke recommends the drafting team clarify the term “malicious activity” as its usage here is very vague and it is unclear how, if at all, it relates back to the types of events in R4.1. (8) Requirement R4.3. Duke suggests rewording this requirement to say, “Activate a response to human detected logging failures before the end of the next calendar day after discovery”. Duke believes that this wording allows the proper flexibility to the entity to begin the clock by which they have to activate a response, no sooner than they become aware of the problem. (9) Requirement R4.4. Duke suggests rewording this requirement to say, “Retain BES Cyber System [sic] logs of events identified in Part 4.1 for at least…”. This wording change clarifies that all logs identified in R4.1 must be retained instead of requiring the entity to assume which ones in R4.1 may actually be related to security events. (10) Requirement R4.5. Duke recommends that the drafting team put additional clarity within the requirement. The current wording is too vague for an entity to determine what is an acceptable summarization or sampling size. Although the Application Guidelines section references a NIST standard for more information, Duke feels the requirement should either be more prescriptive, or clarified that the entity is allowed to come up with its own criteria by rewording the requirement to say, “Review a summarization or

sampling of logged events deemed appropriate by the entity, at a minimum every two weeks to identify undetected Cyber Security Incidents". (11) Measure 4.5. Duke recommends striking the words, "signed and" from the measures section. Suggesting that signed evidence is needed is inappropriate. Having documentation that is dated showing the review should be adequate enough to demonstrate compliance.
(1) Requirement R5.1. Duke requests that the drafting team review the applicability within R5. This requirement does not align with the requirements in CIP-004 to track/manage those with user access. (2) Requirement R5.2. Duke recommends removing this requirement in its entirety. Duke does not believe having CIP Senior Manager authorization of default accounts provides any additional security benefit, nor is it required per an Order 706 directive. (3) Requirement R5.3, Change Rationale. The statement, "Added "authorize" access to make clear that individuals storing, losing, or inappropriately sharing a password is not a violation of this requirement" is too important to leave totally within the Change Rationale section. Duke requests that the drafting team incorporate this verbiage into the requirement as the current word "authorize" does not carry this message on its own clearly. (4) Requirement R5.4. Duke suggests beginning this requirement with "Change known default passwords". Recent news has shown that OEMs often will not disclose the existence of default accounts and the entities should not be held liable when this is the case. Duke also recommends that the drafting team provide clarity on what types of account passwords need to be changed, and that this requirement should only be addressing user or individual accounts and not system accounts. (5) Requirement R5.5. Duke questions the need for a TFE within this requirement. The only circumstances that would warrant a TFE would be identical across the industry for the same devices. Duke does not understand the value that this serves. Duke believes that TFEs should only be needed in unique circumstances and not when a widely-used device is unable to meet the requirements. Duke recommends that the drafting team rework the language within this requirement to not require a TFE, but only that the entity document where passwords cannot be changed due to technical limitations. (6) Measure R5.4. Duke suggests that the phrase "when new devices are deployed" from the first bulleted item. Duke feels that this is redundant, and potentially contradictory, to the implementation plan which describes when an entity must meet compliance with a requirement. (7) Measures R5.5 and R5.6. Duke believes that the second bulleted item should be removed in its entirety. Suggesting that individual attestations would be a good way to demonstrate compliance that the individuals have a password that conforms to policy is inappropriate. Attestations are cumbersome in large organizations and provide no more evidence of compliance than simply providing the password procedure/policy that individuals must conform to. Duke suggests replacing this bullet with the ability to present the procedure/policy as a means to demonstrate compliance. (8) Requirement R5.7. Duke suggests striking this requirement in its entirety. The first means of meeting this requirement, technically limiting the number of unsuccessful authentication attempts actually opens up a vulnerability to a malicious attack by means of a DOS attack. The latter half of the requirement may be partially redundant to requirement CIP-007 R4.2 and may not be technically feasible on all devices. Duke does not believe there is a significant enough increase to security to introduce this requirement and believes it should be removed as it is not specifically required per Order 706.
Individual
Martyn Turner
LCRA Transmission Services Corporation
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

No
Yes
Yes
R1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages.
Yes
Yes
Yes
No
No
In R4.1, we recommend the addition of the term “Where technically feasible” for all of the sub-requirements.
In R5.2, change the wording as follows: The Responsible Entity must document enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). In M5.2, change the wording as follows: Evidence may include, but is not limited to, a listing of enabled default or generic account types in use. R5.3 - Remove the word “authorized” from this requirement. This could be interpreted as requiring an additional authorization for access to these shared or default accounts. R5.4 – Change wording to: Change default passwords where technically feasible.
Individual
Jianmei Chai
Consumers Energy Company
Yes
Yes
Yes
Yes
Yes
Yes
No
R7 – Please provide better definition of “schedule”, “immediate”, and “revocation”, and better examples for each subject. R7.2 - We disagree with the current language because it can unnecessarily restrict the entity from having sufficient transition time between the person leaving and the new person replacing them. The entity should be allowed to specify what their local process is, and timelines, for handling these kinds of revocations to ensure they can plan for continuity of operations properly.
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
Yes
No

R1 – Please provide justification to include physical ports.
R5 - The length of time between password changes in this requirement are excessive. Passwords should be changed far more frequently. Recommend at least quarterly (at least once every 90 calendar days).
Individual
Kayleigh Wilkerson
Lincoln Electric System
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
LES recommends the Applicability columns for the CIP-005-5 Table R2 be revised to exempt non-routable protocol. Suggested wording includes: "High Impact BES Cyber Systems with External Routable Connectivity" and "Medium Impact BES Cyber Systems with External Routable Connectivity".
No
Yes
Yes
Yes
No
Yes
[R1] In all applicability columns for CIP-007-5 Table R1, where medium impact facilities are included, recommend including “with external routable connectivity”. [R2] LES is concerned whether including the monitoring of all installed cyber asset manufacturers is feasible. [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. However, if a company were to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R4.1], the Measure includes the phrase “is capable of detecting”. LES supports this phrase and believes it should be incorporated into the Requirement so companies are not required to replace equipment. Additionally, the “as a minimum” included in R4.1 seems to contradict the understanding of the Measure.
Individual
Joe Petaski
Manitoba Hydro
“BES cyber assets” should be changed to “applicable cyber assets” because the applicability column includes Associated PACS and Associated EACMS.
In Part 1.1 table, “Associated Protected Cyber Asset” is missing. Given that CIP-006-5 doesn’t address that all cyber assets within ESP shall reside within PSP, is it intent that the Protected Cyber Asset within ESP can reside outside PSP?

Group
Arizona Public Service Company
Janet Smith
Yes
No
Yes
Yes
Yes
Yes
No
AZPS recommends moving the statement “Based on their role, some personnel may not require training on all topics” from the rationale for R2 into the appropriate sub-requirements. The intent is to make clear to an auditor that not all topics are required for all roles – and to put that language in the requirements themselves. AZPS recommends changing the words “security controls” in the table 2.2 Measures to “cyber security policies”. AZPS recommends modifying the table 2.3 Measures to make them consistent with those in the table 2.2 Measures. AZPS would like clarity added to the following statement in the table 2.10 Requirements “Training content on risks associated with a BES Cyber System’s electronic interconnectivity and interoperability with other Cyber Assets”. AZPS would like specificity in the table 2.10 Measures to help identify what must be covered in the training materials under requirement 2.10 to be auditably compliant.
AZPS recommends changing the words “next calendar day” in the table 7.2 Requirements to “one calendar week”. AZPS believes a timeline as restrictive as the next calendar day does not provide any value to the overall security posture. Someone transferred to another department, who at one time had a given level of access, does not constitute an immediate threat and in fact having to react in such a manner for the sake of compliance will potentially result in decreased system reliability. Additionally, this is a more stringent requirement than the one for terminations since terminations give additional time for the full revocation of individual user accounts outside of remote access and physical access. Reassignments and transfers are a significantly lower risk than terminations. AZPS recommends adding the words “for reassignments, or transfers” to the table 7.4 Requirements in order to bring the requirements for reassignments and transfers into alignment with the requirement for terminations.
Yes
Yes
No
Yes
Yes
AZPS would like specificity added in the table 1.4 Requirements to define how 99.9% availability should be calculated.
Yes
No
Yes
Yes
Yes
AZPS recommends changing the word “processes” in the CIP-007-5 R2 and M2 statements to “program” in order to match the table 2.1 Requirements.
Individual
Michael Schiavone

Niagara Mohawk (dba National Grid)
Yes
No
Yes
Yes
Yes
Yes
Yes
Regarding R2, we do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training in CIP, as required under the current version, is all that should be required.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement.
Individual
Michael Jones
National Grid
Yes
No
Yes
Yes
Yes
Yes
Yes
Regarding R2, we do not believe that role based training is necessary. The personnel performing the job functions are familiar with the various controls due to their job requirements. General training in CIP, as required under the current version, is all that should be required.
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
No
Yes
The intent of 4.1 as written in the Guidelines and Technical Basis section is inconsistent with the requirement. The guidance states that “It is not the intent that if a device cannot log a particular event that a TFE must be generated”. If the intent is to not be out of compliance when a device cannot log certain events, it should be stated as such in the requirement.
Individual
Jonathan Appelbaum
United illuminating Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
UI concurs with EEi Consensus comments. In addition for R1 UI suggests explicitly stating that this program does not apply to contractors and vendors not directly employed by the Responsible Entity. For R3 The Drafting Team should include a solution for SCADA Support Vendors that require remote access to provide support to the SCADA system, for example ABB support personnel supporting an ABB SCADA environment. It is inefficient to require these vendors to complete every Responsible Entity’s training program. The Draft Standard may provide enough flexibility by allowing an Entity to declare the role of SCADA Support Vendor as requiring no training provided. If the SDT agrees that the flexibility exists then we suggest adding into guidance the concept that SCADA support personnel of the OEM SCADA environment are allowed to forego the Responsible Entity’s training program when performing remote access support functions.
UI concurs with EEi Consensus comments.
Yes
Yes
UI concurs with EEi Consensus comments.
UI concurs with EEi Consensus comments.
No
Yes
Yes
UI concurs with EEi Consensus comments.
Yes
Yes
Yes
Yes
Yes
UI concurs with EEi Consensus comments.
UI concurs with EEi Consensus comments.
Individual

Alice Ireland
Xcel Energy
Yes
Yes
Yes
Yes
Yes
No
No
1) CIP-004-5 R2.2-2.10 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2.1), can a Responsible Entity choose from those elements to create a training program for different roles? Or must all roles identified receive some training from each of the elements in R. 2.2-2.10? If all roles must receive some training for each of the elements in R. 2.2-2.10, what is the value of having role-based training? 2) If all roles must receive some kind of training on all elements of R. 2.2-2.10, we would recommend adding the following language to each of the sub-requirements: Training content should be provided to each identified role based on the level of understanding needed for each. Each identified role must [or must not if Responsible Entities can choose which elements to include] be provided training on this element.
1. The Rationale implies that we need to have our Sr. Mgr. delegate authority to individuals responsible for approving access. Is that the case? 2. The Rationale notes access must be addressed by specific Cyber Asset. Does that mean we need to review/approve access by CA not by location or application/system? 3. R6.2 and R6.3 remove 'for performing assigned work functions' as it is unclear how that would be determined, and subject to different interpretation by the entity and the region. 4. R6.4 remove 'physical and' because it imposes a requirement to create physical access controls and authorization processes to an office that may have a printout of Cyber System Information. 5. R6.7 remove reference in Measures 2 and 3 to 'privileges' as 'privileges' are not mentioned in the requirement. 6. R6.7 clarify Measure 1 – is a 'listing of authorizations' the same as a current list of those with access? 7. R7.2 Rationale and Guideline both indicate that the Review needs to occur by the end of the next day; however the Requirement says that the access must be removed by the end of the next day. We propose allowing 7 days to perform the review, and when access is determined to no longer be required, it be removed by the end of the next business day after that determination is made. It is not feasible to review and revoke access by the next calendar day particularly when you factor in weekends and holidays. 8. R7.3 is not feasible nor is it necessary to act that quickly when we have already disabled remote access (network accounts). A user cannot access a file share without a valid network account. Given the low risk, this timeline is particularly out of line with that imposed in R7.4 which allows 30 days to disable access to CAs. We propose a similar time – 30 days to remove access to Cyber System Information. 9. The Measure for 7.5 does not indicate what would be appropriate evidence for the "extenuating operating circumstances". If documentation is required, the measure should state "Additional documentation for 'extenuating operating circumstances' consists of an overview of the situation, approval by the CIP Senior Manager or delegate, and attestation that the situation has been addressed" or other concrete examples.
No
Yes
The FERC order 706 states that there needs to be an additional level of perimeter protection, but an IDS does not provide protection, just detection. An IPS would allow for protection of malicious software but would require a large investment in personnel and hardware.
None
No
No
No
1) CIP-006-5 R1 states: "Each Responsible Entity shall implement one or more documented physical security plans for its BES Cyber Assets, BES Cyber Systems, Electronic Access Control or Monitoring Systems, Physical Access Control Systems and Protected Cyber Assets that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan.". Xcel Energy requests

clarification regarding the definition of the need for a Physical Security Plan. As stated, it may be interpreted to say that it pertains to each singular cyber asset, system Electronic Access Control or Monitoring Systems and Physical Access Control Systems. Is it NERC's intention to require each entity to provide a singular Physical Security Plan for the above mentioned assets as a single asset? If not, Xcel Energy recommends the language be modified to reflect the need for a Physical Security Plan to include the parts of CIP-006-5 R1, similar to what is in the existing standards. 2) CIP-006-5 R1.3, Xcel Energy seeks clarification regarding additional protection of requiring "two or more different physical access controls". This requirement could result in additional TFEs and add additional management to both the industry and entities. Additionally, most Critical Facilities already contain layered security perimeters, the additional cost of having two factor authentication appears to outweigh the benefit. 3) CIP-006-5 R1.4: the "99% availability" seems both arbitrary and hard to prove (in fact, there are no examples provided in the Measures column for how to prove you have this level of availability). The phrase "with 99.9% availability" should be replaced with language along the lines of "with outages of not more than X per year and of no more than Y minutes duration each allowed." 4) CIP-006-5 R1.7 states, "Issue and alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan…". Xcel Energy seeks clarification on the word "personnel". Could this be a department or does the requirement specify/intend to have entities name each individual? 5) CIP-006-5 R2.1 Measures states, "Evidence may include, but is not limited to, language in a visitor control program…". Xcel Energy seeks clarification concerning a visitor control program. Is it NERC's intent to have an independent visitor control program or is it sufficient to have the language contained within the Physical Security Plan or other procedure? 6) CIP-006-5 R3.1 states, "Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly." The definition of Physical Access Control System does not include the locally mounted hardware. Is it NERC's intent of this requirement to demonstrate maintenance and testing of both the Physical Access Control System and the locally mounted hardware or is the intent that the test of the locally mounted hardware would exhibit that the Physical Access Control System is functioning? Additionally, the Severe VSL for R3 states, "The Responsible Entity has not documented and implemented a maintenance and testing program for Physical Access Control Systems. (3.1)" If the intent of the requirement is to test the locally mounted hardware and the Physical Access Control System(s) it is suggested the language be changed to: "Maintenance and testing of both the Physical Access Control System(s) and locally mounted hardware or devices at the Physical Security Perimeter at least once every 24 calendar months to ensure they function properly." 7) For the measures of CIP-006-5 R3.1, Xcel Energy seeks clarification of what evidence would constitute a "dated maintenance record"? Would a manually created documentation outline illustrating what assets were tested be sufficient or is the electronic record from the Physical Access Control System required? 8) In the Compliance section it states, "The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit. Each Responsible Entity shall retain data or evidence for each requirement in this standard for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer." Since this definition exists in the Standard, is it necessary to indicate on the Requirement level the minimum amount of time to retain records? For example, R1.9 and R2.3 specify retention for 90 calendar days, R3.2 states 12 calendar months.
No
No
Yes
Yes
Yes
1) R1. Not all operating systems will give the RE the ability to disable physical I/O ports, such as USB ports, based upon type usage. Typically, USB ports are disabled by grouping and not by function. If a USB Keyboard and Mouse are used, but other devices are not allowed, then there may be technical feasibility to implement these restrictions. 2) R2. We would dispute the need to create a document every time a patch is released, but rather have a standard process for dealing with released patches

and then document any exceptions to the stated policy. 3) R4.2.1: replace “detected malicious activity” with “detected Cyber Security Incident” 4) R4.5: replace “undetected Cyber Security Incidents” with “potential Cyber Security Incidents not previously identified or detected.”
None
Group
PNGC Comment Group
Ron Sporseen
Yes
Yes
Yes
Yes
Yes
Yes
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes
Individual
John Souza
Turlock Irrigation District
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Individual
Rich Salgo
NV Energy
Yes
Yes
Yes
Yes
Yes
Yes
No
The only disagreement is with R7, specifically part 7.2, as we feel it is impractical to expect that the access requirements of a transferred employee will be assessed in every case within 24 hours of the transfer. We must realize that the employee in question retains the same amount of training and personnel risk assessment before and after the transfer; nothing about the worthiness for access changes as a result of the transfer. We understand the predicament that the SDT has in satisfaction of the Commission directive in Order 706 Paragraph 460 and 461, and believe that the SDT has found an innovative way to accomplish the directive. We simply register our comment about the lack of practicality of the requirement.
Yes
Yes
No
Yes
Yes
In Requirement R1, parts 1.4 and 1.6, rather than specifying a 99.9% availability requirement, we suggest that the requirement be restructured to instead require the implementation of alternate methods to substitute for the loss of any monitoring functionality. Also in Requirement R1, part 1.7, we note that it may be difficult to demonstrate that 15 minutes did not elapse prior to receipt of an alarm, particularly since the alarm is the only data that is captured for evidence. One would assume that the alarm is coincident with the event, but is that sufficient for evidentiary purposes?
Yes
Yes
Yes
Yes
Yes
Individual
Chris Higgins on behalf of BPA CIP Team
Bonneville Power Administration
Yes
Yes

Yes
No
Yes
Yes
No
Regarding R4 – BPA believes the assessment of residence, schooling and employment falls outside the boundary of a criminal history check. Verification of schooling, employments and residence is typically a function of employment eligibility verification and should not be considered a part of the assessment processes for risk associated with access to sensitive areas. Such risk analysis is typically based on character, trustworthiness and any revealed pattern of adverse behavior, which are only able to be assessed in reviewing the criminal history check.
Regarding R7 and R7.1 – BPA believes the requirement is for, “All Terminations” and the requirement does not recognize that not all Terminations are adverse. Contract completions and other similarly non-threatening or non-adversarial ends to employment should not be lumped in with adversarial Terminations or Terminations that create or result from a security risk. BPA believes that the RE needs to have the flexibility to determine whether they feel there is a threat or not. Twenty –four hours should not be applied where there is no threat/risk Regarding R7.2, R7.3 – BPA believes that the, “By the end of the next calendar day” is too aggressive. Essentially it is the same as within 24 hours. When persons are reassigned or transferred it can take a number of days to determine whether they will continue to need the access they previously had. A reassignment or Transfer triggers a series of events such as contact with the loosing and gaining managers, verification of the move, review of the position requirements etc, which will result in a determination of whether the access privileges are necessary or not. There are times when this process of determination may take a week. The previous requirement of 7 days was reasonable and adequate; therefore, BPA suggests returning to that number. R7.4 – BPA believes that, "Revoke individuals users accounts ON BES Cyber Assets" should be changed to "Revoke individuals access TO BES Cyber Assets." BPA believes that this is an important distinction because most field BES Cyber Assets do not have individual user accounts. In the utility field environment many brands and models of devices are being used. For those that do have individual user account capability, they are often not used because most BES Cyber Assets cannot be centrally managed. Since the process of revoking access privileges on each device can take up to a year or longer because it requires a site visit to each asset and for system with a significant number of assets which also covers a large geographic area that effort in combination with the necessary equipment outage to make the change introduces new reliability risks to the BES. It is more common for BPA field organizations to place other access control devices in front of such field devices. These other devices can be centrally managed. So access is controlled to the device rather that by the device itself. Field Example: Protective Relays – Most do not have individual user accounts. Many also do not have the capability to allow central access control management. Because they don't have user accounts the only way to revoke access on the devices is to change the passwords for all access levels. This means logging on to many hundreds to possibly thousands of relays to change passwords. Because access to the relays to change passwords opens the relay at the change level, it presents an increased risk to the BES because it requires a physical equipment outage to make the change resulting in many more outages impacting potentially the state of the BES and once access is granted, one can change any type of setting on the relay . It certainly could not be accomplished in 30 days. Access can be revoked to these assets by revoking the Central Electronic Access Privileges that allow access through the access control devices to the assets. This coupled with physical access revocation (both of which can be centrally managed) provides complete revocation of access to the assets. This can be accomplished a very short time. BPA suggests changing CIP-004 R7.4 to: “For Termination actions, revoke the individuals user accounts on BES Cyber Assets…” to, for termination actions, revoke the individuals access to BES Cyber Assets…” Regarding R7.5 – Most Protective Relays use Access Levels and Codes or Passwords. These are shared among the crews that support the assets. Again as with 7.4 above, this can be hundreds to thousands of devices. Again, BPA believes that this may not be accomplishable within the 30 day time frame.
No
No
BPA finds that there is still confusion regarding how the requirements apply to serial devices. This isn't fully answered in the requirements themselves or the guidance. BPA takes the guidelines for R1

on Page 22, Paragraph 2 to mean that direct serial connected devices are not included in this standard, but further clarification is required. BPA is still uncertain about the intent of the standard in regards to securing serial devices. BPA also understands the requirements as stating that currently no EAPs and thus no ESP boundaries can be defined based on serial communications. This would mean that serial devices or serial communications equipment connected to routable networks within an ESP could possibly extend an ESP far outside the boundaries of a defined PSP. BPA requests that the requirements be changed to address this problem. It is acceptable industry practice to connect control centers to substations and other field equipment using serial communications. The way that CIP 005-5 is currently written could be taken to mean that a control center ESP connected through serial links to various field sites would actually extend the ESP. This could create very large network areas that would have to be compliant. There should be some way to define where an ESP's boundaries are when dealing with serial communications. Not knowing the intent of the SDT, BPA can offer no suggestions. BPA requests that the standard provide examples, if any, of where serial devices would be in scope as well as examples of where serial devices could be used where they are out of scope. Regarding R1.1: The “Applicable BES Cyber Systems and associated Cyber Assets” should use “Medium Impact BES Cyber Systems with External Routable Connectivity” instead of the broader “Medium Impact BES cyber systems”. In addition, it should be made clear in the standard and not just the guidelines that the requirement applies only to Cyber Assets that use a routable protocol. BPA suggests adding “BES Cyber Assets or Associated Cyber Asset that do not use a routable protocol do not have to reside within a routable ESP” to the end of the requirement. Regarding R1.2: BPA supports this requirement. Regarding R1.3: The “Applicable BES Cyber Systems and associated Cyber Assets” should use “Medium Impact BES Cyber Systems with External Routable Connectivity” instead of the broader “Medium Impact BES cyber systems”. In addition, it should be made clear in the standard and not just the guidelines that the requirement applies only to Cyber Assets that use a routable protocol. BPA suggests adding “BES Cyber Assets or Associated Cyber Asset that do not use a routable protocol do not have to reside within a routable ESP” to the end of the requirement. Regarding R1.4: BPA supports this requirement and recommends the removal of "where technically feasible". Regarding R1.5: BPA supports this requirement. Regarding R1 VRFs and VSLs: BPA supports the factors and levels.
Regarding R2.1: BPA believes that the current wording of R2.1 is too vague, too complicated and doesn't adequately provide intent of the guidance. BPA recommends rewording requirement for R2.1 to read: "All Interactive Remote Access must be made through an Intermediate Device that enforces authentication. Direct Interactive Remote Access between a remote Cyber Asset and a BES Cyber System is not allowed." BPA also recommends that guidance lists some of the acceptable Intermediate Devices or methods, such as VPNs, terminal servers, jump boxes, etc. Regarding R2.2: BPA supports this requirement. Regarding R2.3: BPA supports this requirement. Regarding R2 VRFs and VSLs: Yes – BPA supports these factors and levels.
No
Yes
Yes
Regarding CIP-006-5 Table R1: R1, 1.4 and Application Guidelines under R1 specifically referencing opening greater than 96 square inches would be considered an access point. BPA believes that R1-1.4 “99.9% availability” in the current context is unclear to the scope and meaning. For example, does this percentage of availability apply per location, per device or all devices and locations? What is the duration of the reset cycle (i.e., 24 hours, annual)? Does “99.9% availability” only apply to unplanned outages or does this also apply to planned outages? Additionally, if this measure requires evidence that may include and is “not limited to” (i.e., monitoring logs?) documentation to support and/or demonstrate 99.9% availability of the controls that monitor the Physical Security Perimeter (PSP) for unauthorized circumvention of a physical access, does this also imply the need for 99.9% or greater percentage of availability for the reporting/logging mechanism and all of its relevant components? Does “twenty four hours a day, seven days a week” equal or equivalent to “continuous, real-time or perpetual?” For example, a local end-point device may serve as the primary control used to monitor for the circumvention of a PSP; if this device maintains continuous logging (residing in local system memory) within a defined and acceptable availability percentage, does this demonstrate compliance? Attempting to specify a percentage of availability within an undefined process description lacks the necessary context to provide clear guidance at this time. Our recommendation is to provide further clarification to both scope and meaning with detailed provisions allowing for both planned and

unplanned outages. Application Guidelines: The citations used for CAN 0031 and now included in CIP 006 V-5 draft are inappropriate standards for the utility industry. Department of Defense and Central Intelligence Directive sources cited as a basis for the language in CAN 0031, which is now applied to the Guidelines and Technical Basis for CIP 006 Version 5 Draft; are tied directly to that of National Defense and National Security interests (i.e. Nuclear Reactors and Special Nuclear Materials (SNM) and Weapons of Mass Destruction (WMD). Electric utility entities do not posses, process or produce the kinds of information and material intended to be protected by the referenced standards. In no case are public or private utility industry entities operating under a national security classification other than nuclear power facilities which are regulated under other standards. The protection of Special Nuclear Material (SNM), Sensitive Compartmented Information Facilities, (SCIF) and other highly sensitive national security information and material demand standards to prevent intrusions, and unauthorized access to material and information which is not present in the utility environment. The application guideline is attempting to address a vulnerability for which no accompanying risk appears to exist. BPA owns approximately 300 substations located across its service area. BPA's service area includes all or parts of eight western states. A review of security incident records dating back to 2003 show there have not been any intrusions by way of windows, or openings of 96 square inches. (The size of notebook paper)Previous versions of CIP 006 require utilities to implement technical and /or procedural controls to detect and respond to apparent unauthorized access attempts. This version and the cited guidelines are a significant shift in direction moving from "detect" to "prevent" intrusion. This shift in strategy has an exceptional cost impact with little return on investment. The guideline defines an "access point" as any "opening" greater than 96 square inches with one side greater than 6 inches in length. NERC does not provide a definition pertaining to what constitutes an opening. It is essential to know what NERC will consider to be an opening in order for entities to effectively implement the standard. BPA considers an access point as a portal intended for normal human ingress and egress purposes. Without context regarding access points and openings, BPA cannot determine what it will take to become or remain compliant with this requirement. Given the forgoing comments, the needed clarity for the definition of access point, and opening, and unclear indications of what vulnerability is intended to be mitigated by the NERC CIP 006 V.5 Application Guidelines; BPA is voting "No."
No
No
No
No
No
BPA finds it difficult to discuss only the changes made since that last voting period, since not all comments were addressed adequately. These comments address drafts 1 and 2 for all of CIP-007 R1, R2, R3, and R4. Regarding "Background "Applicability Columns in Tables", BPA believes the "Associated Electronic Access Control or Monitoring Systems", "Associated Physical Access Control Systems", and "Associated Protected Cyber Assets" are definitions and should be included in the proposed Definitions, so that entities may comment and vote on them. In addition, BPA believes the term "associated" is too vague. For example, it is difficult to see how an Associated Protected Cyber Asset differs from a Protected Cyber Asset, since in many cases the only "association" would be that Associated Protected Cyber Asset is within ESP, as are all Protected Cyber Assets. Finally, "Associated Physical Access Control Systems" uses the term "External Routable Connectivity", it is unclear whether it is the Physical Access Control System or the BES Cyber Asset that has the External Routable Connectivity, nor is it clear why the other Associated Cyber Assets do not refer to External Routable Connectivity. It is difficult to offer suggestions when we are still unclear on the SDT intent. Regarding 1.1 "Applicability" – BPA believes the 'Medium Impact Cyber Assets' are subject to the requirement only if they have External Routable Connectivity. All Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 1.1 "Requirements" – BPA believes the requirement is not consistent with the Guidelines, which states "If a device has no provision for disabling or restricting logical ports on the device (example - purpose built devices that run from firmware with no port configuration available) then those ports that are open are deemed 'needed.'" That statement modifies the requirement and is inappropriate in a guideline. In addition, including it as part of the requirement would eliminate numerous Technical Feasibility Exceptions. BPA recommends it be moved from the Guidelines to the Requirement. Regarding 2.2 "Guidelines" – BPA

believes the guidelines add additional requirements which are valid and should be in the Requirements. BPA suggests rewriting the Requirements section as “Evaluate the security patches for applicability within 30 calendar days of availability of the patch from the source or sources identified in Part 2.1. The assessment must include determination of the applicability of each patch to the entity’s specific environment and systems as well as reason for a patch’s non-applicability.” Regarding 2.3 “Guidelines” – BPA believes the first sentence of Guidelines restates the Requirement with different wording. BPA is unclear on how this adds new information and believes it gives the appearance of levying an additional requirement. BPA recommends deleting the first sentence of Guidelines 2.3. Regarding 2.4 “Requirements” – If you agree that referring to an existing plan is acceptable than, BPA believes that there is no need to state “For each plan created or revised in Part 2.3…” in the Requirement. BPA suggests “For each plan in Part 2.3…” This would also accommodate the suggested change to R2.3. Regarding 3.1 “Guidelines” – BPA believes the Guidelines make it very clear that the Responsible Entity can determine that a particular Cyber Asset or group of Cyber Assets is not susceptible to malware and needs little or no protection. Regarding 3.1 “Requirements” – BPA agrees with and applauds the decision not to require anti-malware tools on every Cyber Asset. “BES Cyber System” groups Cyber Assets for convenience. R3.1 could be still be construed to apply to each Cyber Asset in the BES Cyber System. BPA believes that R3.1 needs to be explicit. BPA suggests “For Cyber Assets within the scope of CIP-007 R3.1, and which the Responsible Entity has determined to be susceptible to malware intrusion, deploy method(s) to deter, detect, or prevent malicious code. These need not be deployed on every applicable Cyber Asset, as long as each applicable Cyber Asset is protected.” Regarding 3.1 “Measures” – BPA believes that the Measures should be reworded to incorporate the changes to R3.1. BPA suggests rewording as follows “Evidence may include and is not limited to: (1) Documentation of any determinations that specific Cyber Assets or specific types of Cyber Assets are not susceptible to malware and if applicable(2) Records of the Responsible Entity’s deployment of these methods; i.e. through traditional antivirus, system hardening, policies, etc.” Regarding 3.2 “Guidelines” – BPA believes that it should be noted that the Guidelines state, “If a specific Cyber Asset has no updateable software and its executing code cannot be altered…” Since there are other documents associated with Version 5 which clearly implies devices are Cyber Assets only if their executing code can be changed, this is an example of the uncertainty of the definition of “Cyber Asset” and needs to be clarified. Regarding 4.1 “Requirements” – BPA believes that the Requirement does not allow for the SDT intent as stated in the Guidelines. BPA recommends revising the first sentence of the requirement to read “…types of events that the device can log:”. Regarding 4.1 “Measures” – BPA believes the Measures conflicts with the Requirement, unless the Requirement is corrected as identified above. Regarding 4.2 “Applicability” – BPA believes that Medium Impact Cyber Assets are subject to the requirement only if they have External Routable Connectivity. All Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding “with External Routable Connectivity” to the associated Cyber Assets. Regarding 4.2 “Guidelines” – As written, the Requirement does not prohibit the use of procedural controls to achieve compliance. The Guidelines imply that the intent was compliance by technical means. Was that the intent of the SDT? The guidelines and Requirements are not consistent. . BPA suggests that the following sentence be inserted at the start of the Guidelines for 4.2.: “Although manually-generated alerts may be the only means available, automated alerts provide an additional level of security.” Regarding 4.3 “Applicability” – BPA believes Medium Impact Cyber Assets are subject to the requirement only if they have External Routable Connectivity. As the requirement is written, all Associated assets are subject to the Requirement, regardless of connectivity. BPA recommends adding “with External Routable Connectivity” to the associated Cyber Assets. Regarding 4.4 “Requirements” – BPA believes R4.4 still does not prevent a violation for a failure of the logging system. In particular, a hardware failure of media used to store logs would be a violation. In addition, the phrase “where technically feasible” forces Technical Feasibility Exceptions even in the case of a hardware failure of the logging system. This could require after-the-fact submissions of Technical Feasibility Exceptions, which would serve no purpose. Technical Feasibility Exceptions should only be needed in the very rare cases of a logging system that is inherently incapable of providing for long-term retention of logs. BPA suggests rewording as follows: “Unless prevented by a failure of system(s) used for logging, retain BES Cyber System security-related event logs identified in Requirement 4.1 for at least the last 90 consecutive calendar days, where technically feasible.” Regarding 4.5 “Requirements” – BPA believes that, “…at a minimum every two weeks” could be construed as “no less than two weeks apart.” BPA suggests “Review a summarization or sampling of logged events at intervals of no greater than 15 days to identify undetected Cyber Security

Incidents."
BPA recognizes the difficulty of discussing only the changes made since that last voting period, since not all comments were addressed adequately. These comments address all of CIP-007 R5. Regarding 5.1 "Requirements" – Given the extensive comments on CAN-0017 and difficulty in interpreting the draft 1of CIP-007 R5, BPA suggest that the question of technical or procedural controls and the acceptability of procedural controls without technical controls should be explicitly addressed. This is especially important for physical access, where procedural controls such as human guards controlling access are often the best approach. BPA recommends "Using either technical or procedural controls, enforce authentication of all user access, where technically feasible. Technical controls are not required if procedural controls are in place." Regarding 5.3 "Applicability" – BPA believes Medium Impact assets must have External Routable Connectivity to be subject to the requirement. The requirement states that all Associated assets are subject, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 5.5 "Requirements" – BPA believes the suggested password length and complexity are certainly not excessive for password-only authentication. Multi-factor authentication often uses a token and Personal Identification Number (PIN). Such authentication is much stronger than simple passwords, even with numeric-only PINs. Unfortunately, PINs could be construed as a form of password and are subject to R5.5. To clarify the difference, BPA recommends replacing "For password-base user authentication,…" with "For user authentication that uses only passwords…". Regarding 5.6 "Applicability" – BPA believes that Medium Impact assets must have External Routable Connectivity to be subject to the requirement. The requirements states that all Associated assets are subject, regardless of connectivity. BPA recommends adding "with External Routable Connectivity" to the associated Cyber Assets. Regarding 5.6 "Requirements" – BPA recognizes that the requirement has the same issue with multi-factor authentication that R5.5 has. In addition, passwords must be changed every calendar year, not to exceed 15 months. The table that follows R5.5 in the Guidelines suggests changing passwords "During regularly scheduled maintenance" or "During scheduled plant outages" for shared accounts at various locations other than control centers. BPA suggests, "For user authentication that uses only passwords, either technically or procedurally enforce password changes or an obligation to change the password at least once each calendar year, not to exceed 15 calendar months between changes. Changes that can only be performed during regularly scheduled maintenance or scheduled plant outages can be delayed until the next scheduled maintenance or scheduled plant outage, if necessary. Passwords need not be changed if access has been disabled or otherwise prevented until the reinstatement of access." The language change reflects the guidance given in Requirement 5.5's table, where the periodicity of password changes are recommended, and ties it to Requirement 5.6. This suggestion will promote consistency in the Standard. Regarding 5.7 "Requirements" – As noted for R5.1, it is possible that there could be Cyber Assets that do not use technical means of authentication, especially for physical access. As R5.7 is currently worded, this situation would require a Technical Feasibility Exception for lack of technical enforcement of a non-technical control. BPA recommends rewording the requirement to, "For those systems and access for which technical authentication controls are used, and where technically feasible, limit the number…"
Individual
Benjamin Bebernes
Snohomish County PUD
Yes
No
Yes
No
Yes
Yes
No
CIP-004-5 R2 Training should entail security principles not individual processes. The security principles for controlling the BES cyber assets and the storage should be the same. In addition, in most companies the staff isn't this specialized and tends to be supporting everything. Visitors are always escorted, so training should not be required. What could be done is hand them a form to sign that indicates they are entering a BES facility and they are to behave in a certain way (ex. always remain with escort). 2.8 Discusses training on a recovery plan, but what could be more relevant to

keeping the lights on during cyber incidents is the business continuity plan. I would recommend that training occur on the business continuity plan as well or the recovery plan includes the business continuity plan. CIP-004-5 R7, CIP-004-5, Requirement R1, R2, R3, R4, R5, R6, R7 When employees are transferring within a company there may be a need to have a transition period that overlaps with new responsibilities. So how do you define the transfer date? Snohomish would recommend that the access management process include a mechanism for transfers that can document a date that the access will be removed that may be separate from the official start date in new role. The evidence would be the same except the date is the date specified versus the date the person starts new role.
Yes
Yes
CIP-005-5 R1 1.5 requires a method for detecting malicious communication. This should include a “where technically feasible” clause.
Yes
Yes
Yes
Yes
Yes
No
No
No
CIP-007-5 R3 “In Paragraph 622, FERC directs that the requirement be modified to include safeguards against personnel introducing, either maliciously or unintentionally, viruses or malicious software through remote access, electronic media, or other means. The drafting team believes that addressing this issue holistically at the BES Cyber System level and regardless of technology, along with the enhanced change management requirements, meets this directive.” This would require specific policies regarding the use of any type of portable storage such as thumb drives, CD/DVD, portable hard drives, or any other potential storage medium. It would also require specific controls on uncontrolled access to the internet and personal e-mail. The current requirement is way too broad for consistent application. It appears that the requirement has been defined to allow for greater flexibility, however, compliance has been made more difficult by the wording. Documentation every 35 days would be burdensome due to the various signature file updates, OS vendor updates, and control console scanning logs. Use of whitelisting is listed as an option and this has proven technically infeasible for most environments. CIP-007-5 R4 The standard requires manual review of logs, documentation of the review, and an attestation that nothing was identified of a security nature. The sheer volume of logs makes this requirement an audit trap. An automated SIEM is the only real solution and the cost of implementing such a system for a small utility is prohibitive. A documented sampling of logs meets the requirement, but does not provide for any real additional security. This requirement needs more developmental maturity before implementation.
. CIP-007-5 R5 This must include technically feasible on all points due to the nature of the equipment.
Individual
Larry Watt
Lakeland Electric
Yes
Yes
Yes
Yes
Yes
No
No

"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Yes
Yes
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
No
No
No
"Please see comments submitted by FMPA through the formal comment process."
No
Yes
Yes
No
No
"Please see comments submitted by FMPA through the formal comment process."
"Please see comments submitted by FMPA through the formal comment process."
Individual
Ron Donahey
Tampa Electric Company
Yes
No
No
Yes
Yes
No
No
Tampa Electric supports the comments submitted by Edison Electric Institute (EEI). In addition, Tampa Electric is concerned that there will be an administrative burden based on the many versions of training programs tailored to specific roles.
Tampa Electric supports the comments submitted by EEI. Tampa Electric also suggests that the, measures for 6.3 and 6.4 need additional clarification. Tampa Electric is concerned that R6 is an administrative burden with little additional benefit to the security and reliability of the BES. R6.7 is unclear regarding the location.
No
No
Tampa Electric supports the EEI Comments and would appreciate additional clarification related to a proposed definition of “dial-up” connectivity. Should this be defined by what is accessible via the PSTN? Would dial-up (out-of-band) connectivity originating internal to the ESP via a non-public network connection qualify as a dial-up connection that should be afforded CIP005 R1.4 authentication protection? And if so, can the authentication be performed by an intermediary device and pass such credentials allowing for access? For CIP-005 R1.5, please add external routable connectivity to the applicability.
Comments: CIP-005 R2.2 requires encryption for all interactive remote access sessions. Please confirm the interpretation that this requires that only the communication path between the originating device and the intermediary device to be encrypted. For CIP-005 R2.3, Tampa Electric requests the SDT provide clarification related to multi-factor authentication related to whether one-time password (OTP) devices combined with a personal network ID/password combination qualify as multi-factor authentication?
No
No

No
Tampa Electric agrees with the comments provided by EEI. In addition, Tampa Electric raises the following questions. For R1.4: The term “circumvention” is unclear; please provide additional context for improved understanding. For example, how would an entity monitor for this circumvention, for an action like piggybacking or tailgating? R1.4 should include the assets (PACS) that are currently under R1.6. The measure is the same for both R1.4 and R1.6 and requirements are basically the same. This introduces double jeopardy. We also are concerned with the 99.9% availability requirement as stated; this should be struck. It will be difficult if not impossible to track across an entire PACS system (all components). This would not allow for outages and potentially routine maintenance. For R1.3, Tampa Electric requests additional clarification related to the language “two or more different physical access controls” as the current language suggests at two systems to control access into PSP. This could be an issue if guards are not considered adequate to control access to the Control Center (High Impact) PSP. For R1.7 restates R1.5. R1.5 should include the assets (PACS) that are currently under R1.7. The measure is the same for both R1.5 and R1.7 and requirements are basically the same. This introduces double jeopardy Tampa Electric suggests that it is unclear if the Response plan must include a physical presence (human) to respond to an alarm or “Alert.” This requirement as stated also employs circular logic.
Yes
No
Yes
No
No
Tampa Electric supports the comments submitted by EEI. In addition, for CIP-007 R1.2, we request that the SDT provide clarification of physical ports, in particular whether physical ports can be protected via common method (port lock – key), or is there a requirement for unique protections for each port on each device? Tampa Electric suggests that for CIP-007 R2.1, documenting the sources for patches should be a one-time exercise unless additional software is added to the baseline. For CIP-007 R2.3, Tampa Electric requests the SDT provide guidance for procedure if patches cannot be applied, whether technically or operationally not feasible. Would separate TFE/OFEs be required for each exception? Would the TFP/OFE be required once/monthly/annually for the same exception? For CIP-007 R4.2, Tampa Electric requests additional clarification related to alerting for malicious (AV) events. If malicious activity is detected, is an alert required if the entity has automatic controls to quarantine? For CIP-007 R4.3, Tampa Electric requests that the SDT provide clarification on what qualifies as a “response” to logging failures before end of next calendar day. Is it acceptable for the logging failure to be acknowledged even if cannot be corrected by end of next calendar day. CIP-007 R4.5, Tampa Electric requests the SDT to provide guidance requested for what constitutes a “sampling” of logged events… and what evidence should accompany the “review” (logging sample?) It should not refer to an external standard to provide this guidance.
Tampa Electric supports the comments provided by EEI. If the EEI comments are not adopted, Tampa Electric requests clarification for R5.2 on “generic account types” as specific examples of account types are given in the Application Guidelines, p. 46.
Individual
Annette Johnston
MidAmerican Energy Company
Yes
No
No
No
No
No
No
(1) CIP-004 R1 REQUIREMENT: 1) We propose the word “calendar” be deleted to allow entities flexibility of using a different quarterly basis. 2) The word “cyber” should be deleted from the term “cyber security practices” so it is not misunderstood to mean that the scope excludes physical security

topics. (2) CIP-004 R1 GUIDANCE: The following sentence appears to be a statement to the drafting team that should have been deleted: “Guidance: Describe example mechanisms used to demonstrate the availability of this information.” (3) CIP-004 R2 REQUIREMENT: (a) APPLICABILITY: MidAmerican Energy disagrees with the expansion of scope from draft 1 to draft 2 to include associated Physical Access Control Systems and associated Electronic Control or Monitoring Systems in the training requirements. This is an expansion from version 4, which was not directed by FERC. APPLICABILITY: MidAmerican Energy appreciates the addition of “external routable connectivity or dial-up connectivity” in R2 and remaining CIP-004 requirements. (b) In addition, the draft 2 applicabilities for PACS between the standards are not consistent. For example, CIP-006 requires only operational or procedural controls for PACS. Because a PSP is not required for PACS, an entity would not be required to have a list of who has physical access to them, and therefore, would not have a list of who needs training. MEC proposes deleting the PACs and EACs from all of the R2 applicabilities, consistent with scope in V4. (c) R2.1 ROLE-BASED TRAINING: MidAmerican Energy disagrees with the requirement to identify each role and training required for each role, which was not ordered by FERC and is becoming more prescriptive instead of results-based. The requirement is not clear whether one training role and one comprehensive training program for all roles and responsibilities would be acceptable. The rationale infers there must be multiple training modules, which will result in a significant increase in the administrative and documentation burden on entities that have existing training programs. MidAmerican continues to support making the FERC directed changes to version 4, without the significant change to require identification of “each role and training required for each role.” MidAmerican Energy would support deleting R2.1 and changing the R2 statement to include the concept of roles and responsibilities, using language closer to version 4 language, such as: “Each Responsible Entity shall have a cyber security training program to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes the applicable items in CIP-004-5 Table 2 – Cyber Security Training Program, appropriate to personnel roles and responsibilities.” If R2.1 remains, it should clarify that an entity can be compliant if they elect to have one role or elect to have few roles (for example, as a role for those with only physical access, a role for those with cyber access, a role for only information access). (d) R2.2: Revise to: “Training content on the availability of cyber security policies.” There is a significant difference between training content on the policies themselves, vs. the availability of the policies, which is how the requirement should be written, based on its reference of CIP-003-4 R1.2. (e) R2.3: In requirements that include associated systems (which are not BES Cyber Systems), the text of the requirement should reference “applicable Cyber Assets” instead of BES Cyber Systems. We have recommended associated systems be removed from the applicability, but if this change is not made, this requirement should be changed to: “Training content on the physical access controls protecting the applicable Cyber Assets.” (f) R2.5: MidAmerican does not object to this requirement, but the change rationale of “no significant change from previous versions” is incorrect since visitor control program was not included in the training requirements in version 4. (g) R2.6: no comments (h) R2.7: The wording is too prescriptive. Change to: “Training content on BES Cyber Security Incidents” and then delete R2.9. (i) R2.10: Revise the wording to eliminate conflicts with applicabilities and still meet FERC language concepts from paragraph 434: “Training content on security risks associated with networking hardware and software electronic interconnectivity and interoperability.” Good draft two includes the word “risks.” Add “security” to risks and be sure to retain. This is a good change the clarifies the training is on risks, not on how to interconnect networks. (4) CIP-004 R2 GUIDANCE: The following sentence appears to be a statement to the drafting team that should have been deleted: “Provide guidance or a local definition of “role appropriate” as it is used in the standard.” Add the statement in guidance such as: “It is acceptable to have one training program covering all of the required topics, if an entity chooses to provide the same program to all authorized personnel covering all roles and responsibilities.” See also comments on R2.1 (5) CIP-004 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, to prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R3.1: Delete “and documentation” from the requirement. The requirement should be to complete the training before access is used. Documentation is covered by the measure. This should not be considered a violation. We have recommend associated systems be removed from the applicability due to scope expansion. “BES Cyber Systems” should be changed to “applicable Cyber Assets” in the requirement text. (c) R3.2: Delete “and documentation” from the requirement. Documentation is covered by the measure. (d) ANNUAL: Revise “at least once each

calendar year, not to exceed 15 calendar months," to "once each calendar year or a period not to exceed 15 calendar months between training." (6) CIP-004 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. CIP-004 R3 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (7) CIP-004 R4 REQUIREMENT: (a) R4 requires a personnel risk assessment program. We propose the R4 parts be written parallel to the parts in R2, which requires a training program. See following comments. (b) R4.1 proposed text: "Program content on an initial personnel risk assessment that includes identity verification. (c) R4.2: Delete the following text: "4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable)." The deleted text could be moved to guidelines. The text was from failed interpretation 2009-23. Since the industry rejected this text, it should not be included in version 5. This text is too prescriptive and not in response to a directive. We propose the following text for R4.2: "Program content on seven year criminal history records check. If it is not possible to perform a full seven year criminal history records check, conduct as much of the seven year criminal history records check as possible and document the reason the full seven year criminal history records check could not be performed." (c) R4.3: Revise to: "Program content on a process or criteria to evaluate personnel risk assessments to determine when to deny authorized access." (d) R4.4: Revise to: "Program content on a process or criteria for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3." Or alternatively, delete the requirement as duplicative of those parts and clarify in the R statement above the table that it R4 applies to all personnel, including contractors or service vendors. (8) CIP-004 R4 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (9) CIP-004 R5 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, to prevent recurrence of flaws. Expeditiously corrected flaws are not violations. (b) R5.1 REQUIREMENT: Revise the text to make it clear that the PRA must be performed before the first authorization. The following text is proposed: "Have a personnel risk assessment prior to accessing applicable Cyber Assets, except for CIP Exceptional Circumstances. Subsequent authorizations within the life-time of PRAs do not require repeating the background check." (10) CIP-004 R5 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. (11) CIP-004 R5 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.

(1) CIP-004 R6 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, to prevent recurrence of flaws. (b) R6.1 Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. R6.1.2: Revise to "unescorted physical access into a PSP" since it is possible to authorize access for a PSP. Associated PACS do not require a PSP. (c) R6.2: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. Although the word "minimum" was deleted from draft 2, we still think there is too much ambiguity with the phrase "necessary for performing assigned work functions" and it should be delted. We propose revising this requirement to: "The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances." (d) R6.3: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. To eliminate ambiguity, we propose replacing the term "necessary for performing assigned work functions," with "appropriate." (e) R6.4: Delete "or dial-up connectivity" from the applicability to be consistent with applicabilities on other standards. To eliminate ambiguity, we propose replacing the term "necessary for performing assigned work functions," with "appropriate for the roles and responsibilities." (f) R6.5 AND R.6.6: MidAmerican commented on draft 1 that R6.5 and R6.6 are major scope expansion not directed by FERC. The SDT responded that the changes were made because of past industry comments that "review the list of its personnel who have such access" is not well understood or consistently implemented. We continue to feel the requirements are not just clarification, but are expanding scope, as well as overlapping requirements between R6.5 and R6.6. The additional administrative work created is not offset by a commensurate improvement in security. MidAmerican proposes supports and will participate in

working toward language to alleviate these concerns. (g) R6.5/R6.6 APPLICABILITIES: Delete “or dial-up connectivity” from the applicability to be consistent with applicabilities on other standards. (h) R6.6: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between verifications,” to “once each calendar year or a period not to exceed 15 calendar months between verifications.” (i) R6.6 REQUIREMENT: Change “performing assigned work functions” with “are appropriate.” R6.6 MEASURES: Replace the numbered list with bullets and “or.” (j) R6.7: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between verifications” to “once each calendar year or a period not to exceed 15 calendar months between verifications.” R6.7 REQUIREMENT: delete “minimum” since it was deleted in the requirement. R6.7 MEASURES: Change numbered list to bullets with “or.” Delete “any” in the measure. Revise the measures to correspond to other changes listed above. (2) CIP-004 R6 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-004 R7 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, to prevent recurrence of flaws. (b) Immediate revocation of access is listed on the EEI REAC key issue list. Though FERC Order 706 mandated “immediate” revocation, many entities consider the scope of cyber assets in the applicability too broad and problematic. We think two changes balance security and resource requirements: (i) Incorporate the language suggested that allows detection and correction without it being a violation. (i) Limit the immediate revocation to high impact BES Cyber Systems, and allow additional time for the other asset categories. MidAmerican suggests limiting the draft 2 R7.1-R7.3 to High Impact BES Cyber Assets which may require writing new parts for the medium impact BES Cyber Assets. Requirements for medium should not increase the current version 4 compliance thresholds. (c) R7.4 and R7.5 already are limited to high impact, which we agree with. Another major issue of concern to the industry is access revocation of contractors. Draft 2 does not specifically address differences in the requirements based on employees vs. contractors. We would like to work with the SDT to find some solutions to this issue. (d) R7.1 REQUIREMENT: Change the requirement text to identify the time the termination action is communicated to address concerns regarding notification of terminations that are predated or retroactive. Proposed text: “For all termination actions, initiate the process to revoke the individual’s unescorted physical access and Interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action.” (d) R7.1 MEASURES: Change the numbered list to bullets with “or.” Add a measure for completion, since the measures listed are for initiation. (e) R7.2: Change the requirement text to incorporate the initiation of revocation, along with the determination that access is no longer needed. Proposed text: “For reassignments or transfers, initiate revocation of the individual’s electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary.” Change the numbered list to bullets with “or.” Add a measure for completion, since the measures listed are for initiation. (f) R7.3: We propose this be limited to terminations for cause for employees. We think additional discussion is needed for contractor processes. Change the requirement text to incorporate the initiation of revocation. (g) R7.4: No comments. (h) R7.5: Add “to BES Cyber Assets” to the requirement to align with R7.4 which includes the phrase: “For termination actions, reassignments, or transfers, change passwords for shared account(s) to BES Cyber Assets known to the user within 30 calendar days of the termination action, reassignment, or transfer of the user.” (4) CIP-004 R7 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

(1) CIP-005 R1 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, to prevent recurrence of flaws. (b) R1.1: APPLICABILTY: MidAmerican Energy recommends the applicability for 1.1 be High Impact BES Cyber Systems with External Routable Connectivity, Medium Impact BES Cyber Systems with External Routable Connectivity and Associated Protected Cyber Assets. This

moves the external routable qualifier out of the requirement into the applicability where it belongs and makes 1.1 parallel to 1.2. (c) R1.1 REQUIREMENT Proposed Text: “Applicable Cyber Assets shall reside within a defined ESP.” The proposed changes move text referencing applicability to the applicability part of the table. This also removes text from the requirement that is redundant to the definition of ESP (see comment above). (d) R1.2 REQUIREMENT Proposed text: “All External Routable Connectivity must be through an identified Electronic Access Point (EAP).” By definition, external routable connectivity ties the ESP to the Cyber Asset so the reference to ESP is circular when the definition of NERC is applied. This also eliminates the use of “through” twice in the same sentence. (e) R1.3 No comments. (f) R1.4 MidAmerican Energy recommends this requirement be deleted. Dial-up authentication belongs in table 2 for interactive remote access management. Table 2 already has requirement 2.3, which requires authentication for Interactive Remote Access. (g) R1.5 MEASURES: Change “and” to “or” and use bullets for 1. and 2. The two sub bullets for 1. could be separated so there are three bullets as examples. (2) CIP-005 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-005 R1 VRF: In its May 18, 2007 order on violation risk factors, FERC identified five guidelines for approval of VRFs, including consistency among reliability standards. After reviewing VRFs on all existing NERC standards, MidAmerican Energy Company is proposing a change to the VRFs on several of the version 5 draft 2 requirements, including CIP-005 R1. We agree the VRF should be medium for the high impact BES Cyber Systems, but we think the VRF should be lower for the medium impact BES Cyber Systems.
(1) CIP-005 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, to prevent recurrence of flaws. (b) R2.1-2.3APPLICABILITY: MidAmerican recommends adding “with External Routable Connectivity” for each applicability because it directs this requirement to the greatest risk and where there are the greatest security benefits to be achieved and the most mature technology. BES Cyber Assets in medium dial up accessible substations pose less risk and technology is not as proven. The applicability should be compared to proposed changes to relevant definitions where the proposal is remove dialup from the definition(s). (c) R2.1 REQUIREMENT Proposed text: “Restrict Interactive Remote Access to only authorized users such that the Cyber Asset initiating Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset.” This does not prescribe how technologically to accomplish this and allows for application proxy firewalls. (d) R2.3 REQUIREMENT: see applicability comment for externally routable. (e) As recommended in R1, move CIP-005 R1.4 for dial-up authentication to R2 and incorporate multi-factor authentication. This eliminates redundancy and double jeopardy. Add “where technically feasible.” (2) CIP-005 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. (3) CIP-005 R2 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems.
No
No
No
(1) CIP-006 R1 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, to prevent recurrence of flaws. (b) R1.1: No comments. (c) R1.2: No comments. (d) R1.3: The SDT states in its consideration of comments that changes were made to clarify that two different physical access controls are required, not two completely independent physical access control systems. However, there still has been considerable discussion on what is meant by this requirement during industry association meetings. Clarify the requirement by adding a sentence, such as the statement in the consideration of comments: “Two different physical access controls are required, not two completely independent physical access control systems.” The guidance is clear, for example, that bio and PIN is okay. This reflects the concept in the requirement which will be enforced. (e) R1.4 and R1.5: V4 required monitoring of PSP access points. V5 eliminates the concept of access points and six-wall borders. R1.4 and R1.5 require monitoring for “unauthorized circumvention of a physical access

control into a PSP" and issuing an alarm "in response to detected unauthorized circumvention of a physical access control into a PSP." This could be read to mean monitoring and alerting of the entire PSP, such that video and/or motion detection would be needed for compliance. We understand the intent of the SDT in adding the 99.9% availability in R1.4; however, we think it would require extensive documentation to track compliance. Our proposed text in the R statement above the table will address the concern with zero defect compliance with this requirement, without less documentation burden. We propose combining R1.4 and R1.5 into the following revised text that addresses the concerns with monitoring the PSP. We suggest replacing the term "monitor" with "alert" since the intent is to provide alerts: "Have controls that provide alerts for detected unauthorized circumvention of physical access controls for the Physical Security Perimeter. Respond within 15 minutes of detection of unauthorized circumvention of a physical access control. If a six-wall border is established for the PSP, alerting is only required for access points into the PSP. If a six-wall border is not established, alerting of the entire PSP is required." (f) R1.6 and R1.7: Combine these parts, remove the 99.9% availability reference and replace "monitor" with "alert." The following text is proposed: "Have controls that provide alerts for detected unauthorized circumvention of physical access controls for the Physical Access Control Systems. Respond within 15 minutes of detection of dtected unauthorized circumvention of physical access controls to a Physical Access Control System." (g) R1.8: No comments. (h) R1.9: No comments. (2) CIP-006 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-006 R1 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (4) CIP-006 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, to prevent recurrence of flaws. (b) R2.1: The addition of the words "who are known or guests and" makes it sound like guests are unknown people. We think the requirement is clear with the following text: "Require continuous escorted access of individuals not authorized for unescorted physical access, except during CIP Exceptional Circumstances." (c) R2.2: No comments. (d) R2.3: No comments. (5) CIP-006 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. CIP-006 R2 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (6) CIP-006 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, to prevent recurrence of flaws. (b) R3.1: Change all references (within the applicability, requirement, measure and guidance) from "locally mounted hardware or devices" to "locally mounted devices." The guidance states that testing includes motion sensors, electronic lock control mechanisms and badge readers, which most people would not think of as hardware. Hardware could be interpreted to include door hinges and screws, which should not be included in the requirement. (c) R3.2: In applicability, change "locally mounted hardware or devices" to "locally mounted devices." Change the text requirement to focus on the defined term: "Document outages for Physical Access Control Systems and retain the outage records for at least 12 calendar months." Or, alternatively, move the document retention to the Compliance section C. (6) CIP-006 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
No
No
(1) CIP-007 R1 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, to prevent

recurrence of flaws. (b) R1.1 REQUIREMENT: Add the following statement to the requirement text: “If a device has no provision for disabling or restricting logical ports on the devices, then those ports that are open are deemed necessary.” Add the following guidelines: “An example of a device that has no provision for disabling or restricting logical ports on the devices are purpose built devices that run from firmware with no port configuration available.” (c) R1.1 MEASURES: Add a fourth bullet to address CIP-005-4 R2.2: Listing of access points to the Electronic Security Perimeter(s), including configuration of ports and services, individually or by specified grouping. (d) R1.1 GUIDANCE: Remove the reference to CIP-005 R1 to protect the network, since this isn’t applicable with version 5. 3) R1.2: Revise the text to begin with “Have methods to protect against…” since the VSL is for not having methods. (2) CIP-007 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-007 R1 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (4) CIP-007 R2 APPLICABILITIES: Add “External Routable Connectivity” to the Medium Impact BES Cyber Systems for all of the parts of R2. The security risk level is different on purpose built Cyber Assets that don’t have external routable connectivity or dial up accessibility. Focus resources on the higher risks. (5) CIP-007 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, to prevent recurrence of flaws. (b) R2.1 REQUIREMENT: We think it is important to include security upgrades in this requirement. We propose the following text to make it clear that upgrades are included: “A patch management program for tracking, evaluating, and installing cyber security patches and security upgrades for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches and security upgrades for applicable Cyber Assets that are updateable and for which a patching or upgrade source exists.” (c) R2.2 REQUIREMENT: We appreciate the change that was made in CIP-007 R3.3 to allow 35 days and request R2.2 to be changed to 35 days to allow the normal monthly update cycles to have a chance to execute. (d) R2.3 REQUIREMENT: As stated in R2.1, we think it is important to include security upgrades. Change “applicable patches” to “applicable security patches and security upgrades.” Change “security patch” to “security patch or security upgrade.” We believe the primary focus should be on installing the security patches or upgrades and moderating the amount of documentation. (For example, about 160 Windows based Cyber Assets have 84,000 distinct patch assessment outcomes, a subset, but significant scale of which require installation. We suggest changing to 60 calendar days and adding the following sentence to the requirement: “a remediation plan is not required for security patches or security upgrades installed within 60 days of release from the identified source.” This incents prompt implementation which is good for security and reduces paperwork which frees resources for other security adding work. Delete or revise the word “dated” since the guidance suggests a plan could be based on the next outage. (e) R2.4 REQUIREMENT: We appreciate the flexibility provided in R2.3, including the possibility of an “open ended” plan similar to a TFE without an expiration date. However, we think additional flexibility is needed to allow the plans to be revised. As written, R2.4 does not allow the plan to be revised, except in CIP Exceptional Circumstances. NERC has recognized the need for entities to make changes to implementation plans, such as with TFEs. Revise the requirement to: “For each plan created or revised in Part 2.3, implement the plan, except for CIP Exceptional Circumstances. If the plan cannot be implemented within the timeframe specified, revise the plan before the timeframe expires and implement according to the revisions.” (6) CIP-007 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. (7) CIP-007 R2 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower. (8) CIP-007 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, to prevent recurrence of flaws. (b) R3.1 REQUIREMENT: MidAmerican provided comments on draft 1 that the requirement needs to be clear on the competency based approach. There is some excellent description of this, but it is only in the summary of changes and application guidelines, which are not enforceable. We proposed the following revised text: "Deploy method(s) to deter, detect, or prevent malicious code based on the Cyber Asset's susceptibility to malware. Methods do not have to be used

on every single Cyber Asset." In the consideration of comments, the SDT stated that adding "susceptibility" to the requirement is another element that could require some form of evidence from every entity for every Cyber Asset. The SDT further states the requirement is "applicable at the systems level, so that every Cyber Asset is not included." However, this requirement also applies to Associated Protected Assets, which is at the asset level. We continue to have concerns that the requirement, as written, does not clearly state that methods are not required on every asset. We would appreciate the opportunity to discuss acceptable solutions with the SDT. One idea would be to add the following sentence to address the associated protected Cyber Assets: "Associated protected Cyber Assets may be included in the methods for the BES Cyber Systems with which they are associated." Perhaps a better solution proposed in other MidAmerican comments is to rephrase the applicability, such as, "high impact BES Cyber Systems, including Associated Protected Cyber Assets." (c) R3.1 GUIDANCE: The last sentence in the R3.1 section of the guidance has a statement "should not require a TFE." This makes it sound like there is an option for a TFE. Reword to make it clearer that TFEs are not available and not needed. (d) R3.2 REQUIREMENT: Add the following sentence: "Mitigation for the Associated Protected Assets may be accomplished through other applicable systems." (e) R3.3: No comments. (9) CIP-007 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. (10) CIP-007 R3 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems. (11) CIP-007 R4 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, to prevent recurrence of flaws. (b) R4.1: Many in the industry requested that the requirement be revised to make it clear that TFEs are not needed if a device cannot log. In its consideration of comments, the SDT stated TFE exclusion language is not necessary but attempted to strengthen the basis for not requiring TFE exclusion language. MidAmerican Energy believes that adding TFE exclusion language will eliminate the need for discussion on this in the future, especially with auditors. Since there continue to be questions from many entities about the meaning of the requirement, we again suggest the following sentence be added to the requirement: "Devices that cannot log a particular event do not require a TFE to be generated." (c) R4.2 REQUIREMENT: We continue to have concern with the use of the term "real time" and don't think the changes addressed this concern. The term "real time" has an implied meaning in the industry, and it's not used in that manner within this requirement. This requirement exceeds the scope of version 5 without a FERC directive, and draft 2 has become more prescriptive with the listing of the types of events. In its consideration of comments, the SDT states "This is not a requirement that the systems or assets themselves perform an alert, but rather a requirement that the entity implement a method to produce a real-time alert upon detection of the stated conditions." However, the requirement, as written, does not match the SDT's explanation. We would propose the requirement be revised to better reflect the SDT's intent: "Have methods to generate alerts, where technically feasible, for events that the Responsible Entity determines necessary." "Malicious activity" in R.4.2.1 should be "security event," if this item remains in the requirement. (d) R4.3 REQUIREMENT: Add "after detection" at the end of the sentence. (e) R4.4 REQUIREMENT: Change to "Retain BES Cyber System and BES Cyber Asset…" R4.4 MEASURES: Change number list to bullets with "or" in between. (f) R4.5 APPLICABILITIES: Change the applicabilities to "High Impact BES Cyber Systems, including Associated Protected Cyber Assets." This clarifies that logging reviews do not apply at the asset level. Exclude the Associated Electronic Control or Monitoring Systems and Associated Physical Access Control Systems. (g) R4.5 REQUIREMENT: Revise the text to make it clearer that the entity determines which logs should be reviewed or sampled. Proposed text: "Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum every two weeks to identify undetected Cyber Security Incidents." (12) CIP-007 R4 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. (13) CIP-007 R4 VRF: To be consistent with other reliability standards, we think the VRF should be revised from medium to lower.

(1) CIP-007 R5 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, to prevent

recurrence of flaws. (b) R5.1 APPLICABILITIES: The applicabilities in CIP-007-5 R5 should be consistent with those in CIP-004-5 R6 and R7. Therefore, change “medium impact BES Cyber Systems” to “medium impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity.” (c) R5.2 REQUIREMENT: This requirement should be deleted since it duplicates CIP-004 R6.2, creating double jeopardy. When we designated an approver in CIP-004, it also covers accounts. In addition, the requirement still has the CIP Senior Manager authorization, even though consideration of comments indicates it was removed. (d) R5.3: This requirement should be deleted since it duplicates CIP-004 R6, creating double jeopardy. If the SDT believes the requirement is necessary, we request an explanation of the difference between this requirement and CIP-004-5 R6.2. The following concept from the rationale is good information and should be incorporated within CIP-004 or elsewhere, if this requirement is deleted: sharing of password is not a violation. (e) R5.4 REQUIREMENT: : Consider changinge “default passwords” to “known user default passwords” or clarifying what passwords are included in this requirement. Start with the TFE phrase. The placement of “technically feasible” in draft two creates some confusion. (f) R5.4 MEASURES: Delete: “when new devices are deployed” because timeframes are covered in implementation plan. (e) R5.5: No comments. (f) R5.6: ANNUAL: Revise “at least once each calendar year, not to exceed 15 calendar months between changes,” to “once each calendar year or a period not to exceed 15 calendar months between changes.” (g) R5.6 REQUIREMENT: Some assets may not be capable of password changes, either technically or operationally. We suggest the following revised text to address this concern but eliminate the need for a TFE (with the proposed changes, the phrase “or obligation to change the password” can be deleted): “For password-based user authentication, either technically or procedurally enforce password changes, within capabilities of the device or operational requirements, at least once each calendar year, not to exceed 15 calendar months between changes.” (h) R5.6 GUIDANCE: The table has not been updated. (i) R5.7 REQUIREMENT: This new requirement was not directed by FERC and it overlaps with CIP-007 R4.2, presenting the possibility of double jeopardy. It also will likely generate many TFEs. We think it should be deleted, and information regarding the number of unsuccessful login attempts could be added to the guidance of CIP-007 R4.2. If the requirement is not deleted, it should be revised to eliminate any overlap with R4.2. Text could be revised to: “Limit, where technically feasible, the number of unsuccessful authentication attempts, unless an alert is generated for R4.2.” (i) R5.7 GUIDANCE: There is no guidance provided for this requirement. (2) CIP-007 R5 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-007 R5 VRF: We agree the VRF should be medium for the high impact BES Cyber Systems. To be consistent with other reliability standards, we think the VRF should be lower for the medium impact BES Cyber Systems.
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
The intent of R4.2 is not clear. If the intent is to require criminal history checks from every location where an individual has lived or worked regardless of official residence, we suggest the following wording: “4.2.1. resided; or 4.2.2 been physically located for employment ; or 4.2.3. been physically located to attend school.” This would also appropriately exclude remote employment and on-line classes.
Yes
No
“Intrusion detection system” has a specific connotation in the computer security community. For the Measures for R1.5, we recommend changing “intrusion detection system” to “detection system” to be in line with the requirement and allow for various appropriate technologies for complying with the

requirement.
Change R2.3 to read “Require multi-factor authentication for all Interactive Remote Access sessions.” Move bullets to the Guidelines. Multi-factor authentication is well understood in the computer security community.
Yes
Yes
No
(Comment 1) The definition for “Locally mounted hardware or devices at the Physical Security Perimeter” (last paragraph of the Background section, page 8) expands upon the definition of Physical Access Control System. A badge reader that stores data and independently performs access authentication would not likely be vulnerable to tampering and would pose less risk than a badge reader that could be remotely accessed through a network. Suggest striking “does not contain or store access control information or independently perform access authentication“ and replacing with “does not communicate using a routable protocol.” (Comment 2) In Measures for 1.2 and 1.3, recommend striking “card reader” from the phrase “card reader logs.” (Comment 3) In Measure for 1.6, please replace both instances of “Physical Security Perimeter” with “Physical Access Control System” to align with the requirement.
Yes
No
Yes
No
No
(Comment 1) Implementation plans must be revised sometimes due to testing results, new information or operational factors. In R2.4, do "CIP Exceptional Circumstances" provide entities with the latitude to revise implementation plans and timeframes if necessary? If not, please add the following to R2.4, "Document the execution status of any remediation or mitigation action items, including any changes to the plan or timeframe." (Comment 2) R4.1 – recommend changing “each of the following types” to “each of the following types that the system is capable of detecting and logging” in order to clarify SDT’s intent as indicated in both the Measure and the Guidance. (Comment 3) Measure for 4.3, suggest replacing “events” with “failures” for clarity.
For clarity, suggest changing R5.7 to read “Generate alerts after a threshold of unsuccessful login attempts or limit, where technically feasible, the number of unsuccessful authentication attempts.”
Individual
Jim Howard
Lakeland Electric
Yes
Yes
Yes
Yes
No
No
No
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
Yes
Yes
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
No
No
No

see comments submitted by FMPA through the formal comment process
No
Yes
Yes
No
No
see comments submitted by FMPA through the formal comment process
see comments submitted by FMPA through the formal comment process
Group
Dominion
Connie Lowe
Yes
No
No
No
Yes
No
No
CIP-004-5 R2 - The language in 2.9 (Training content on response to BES Cyber Security Incidents.) dupicates a portion of the language in 2.7 (Training content on identification of a potential BES Cyber Security Incident and initial notifications in accordance with the entity's incident response plan). Part 2.9 should be deleted in its entirety. CIP-004-5 R3 - Part 3.1 should be revised to remove the "and documentation" wording documentation is a measure and proof of compliance of execution of the requirement. Also, training is required prior to granting authorized unescorted physical access OR authorized electronic access. The proposed wording is: "Require completion of the training specified in CIP-004-5, Requirement R2 prior to granting authorized electronic access or authorized unescorted physical access to applicable systems, except during CIP Exceptional Circumstances." CIP-004-5 R4 - The first sentence of Part 4.2 should be revised to "consecutive" months for clarity as follows: "Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more:" - In Part 4.4, the order of the words "criteria" and "process" is inconsistent with Part 4.3. For consistency, the words in the requirement should be reordered as follows, "Process or criteria for verifying that personnel risk assessments performed for contractors or service vendors are conducted pursuant to CIP-004-5 R4, Parts 4.1 through 4.3"
CIP-004-5 R6 - Part 6.1 should allow for role-based designations. The first sentence should be revised as follows, "Designate one or more individual(s) or role(s) to authorize:" - Part 6.2 can be simplified for clarity and intent by removing the clause "required work functions". The language of the requirement should be changed as follows, "The individual(s) or role(s) designated in Part 6.1 shall authorize electronic access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." - Part 6.3 can be simplified for clarity and intent by removing the clause "required work functions". The language of the requirement should be changed as follows, "The individual(s) or role(s) designated in Part 6.1 shall authorize unescorted physical access deemed necessary by the Responsible Entity, except for CIP Exceptional Circumstances." - Part 6.4 needs to be clarified; electronic "locations" is not a typical term and should be replaced with "repositories". The language of the requirement should be changed as follows, "The individual(s) identified in Part 6.1 shall authorize access to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances." - Part 6.5 should be limited to individuals who are CURRENTLY provisioned to limit the scope of the review. The review isn't intended to perform a reconciliation of all individuals who may have gained and lost access during the review period. The language of the requirement should be changed as follows, "Verify at least once each calendar quarter that individuals currently provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records" - Part 6.6 is too broad by using the

word "all" with regard to user accounts rather than "applicable". The language of the requirement should be changed as follows, "For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all applicable user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions." - Part 6.7 needs to have the word "privileges" inserted into the stated requirement after the word "access" to be consistent with the change rationale as well as have confirming language applied to electronic "locations". The language of the requirement should be changed as follows, "Verify at least once per calendar year, but not to exceed 15 calendar months between verifications, that access privileges to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions." CIP-004-5 R7 - Part 7.3 should be updated with conforming language using the term "repositories" as a result of changes suggested for previous requirements as follows, "For termination actions, revoke the individual's access to the designated physical and electronic repositories where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action" - Part 7.4 Applicability should include "Medium Impact BES Cyber Systems with External Routable Connectivity or dial-up connectivity" for consistency with 7.1 through 7.3 CIP-004-5 GUIDANCE - Access revocation timing requirements associated with the death of an employee should be treated similar to a 'normal' termination and not be treated similarly to a 'for cause' termination.

No

No

CIP-005-5 R1 - The applicability column for Part 1.1 should include the items in Part 1.2 which are High Impact BES Cyber Systems with External Routable Connectivity, Medium Impact BES Cyber Systems with External Routable Connectivity, Associated Protected Cyber Assets applicable to High and Medium Impact BES Cyber Systems with External Routable Connectivity. - The requirement for Part 1.1 should remove the reference to Associated Protected Cyber Assets. The revised language of the requirement is, "All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. " - The Measure for Part 1.1 includes all Cyber Assets, but the Applicability includes only BES Cyber Systems. Either the Applicability needs to be extended to Associated Protected Cyber Assets or the Measure needs to be restricted to BES Cyber Systems.

CIP-005-5 R2 - The "Technical Feasibility" language is included in the header of standard (which is about developing processes) and seems to imply that technical feasibility exceptions can be taken for any of the Parts. It isn't possible to take a technical feasibility exception for the development of a process; however, it is possible to take a technical feasibility exception for the technical components required in the Parts to the Requirement. For clarity, we recommend the technical feasibility language be applied to each of the Parts of the requirements (see examples below) and removed from the header. The proposed language for the requirement is, "Each Responsible Entity allowing Interactive Remote Access to BES Cyber Systems shall implement one or more documented processes that collectively include the applicable items...". - Part 2.1 requires clarity because cyber assets themselves cannot initiate Remote Interactive Sessions. The language of the requirement should be simplified to, "Utilize an Intermediate Device such that the Interactive Remote Access does not directly access a BES Cyber System or Protected Cyber Asset, where technically feasible." - In Part 2.2 the portion of the sentence after "intermediate device" is editorial and can be moved to Application Guidance as it doesn't add value to the requirement. The language of the requirement should be changed to "Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device, where technically feasible."

No

No

Yes

CIP-006-5 ALL - Parts 1.2 and 1.3 as worded would prevent an escorted person from entering the PSP. The language of the requirements needs to be clear that escorted individuals are able to enter a PSP. The phrase "and their associated visitors" should be added to the end of each of the requirements to correct. As an example, Part 1.2 would be rephrased as " Utilize at least one physical access control to allow physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access and their associated visitors." - The

measures of Parts 1.2 and 1.3 need to be updated to reflect escorted visitor access. The language of the measure should be changed as follows, " Evidence may include, but is not limited to, language in the physical security plan that describes each Physical Security Perimeter and how access is controlled by one or more different methods and proof that access is restricted to only authorized individuals, such as a list of authorized individuals accompanied by card reader logs and/or visitor logs." - The degree to which the controls in Part 1.4 aren't clear and when combined with the 99.9% availability, make the Part impossible to comply with. For example, an entity might have to monitor for individuals breaking through a concrete block wall or digging a tunnel to break in through a floor. "Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter." We suggest the language be reverted to the language in CIP006-4c, R5. - Part 1.5 should be changed for clarity by replacing the words "unauthorized circumvention" with "tampering". The revised language of the requirement should be "Issue an alarm or alert in response to detected tampering of a physical access control into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection." - Parts 1.6 and 1.7 can be merged into Parts 1.4 and 1.5 respectively. - Change Part R1.7 to "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the detection of unauthorized access." The word "detection" is required to clarify when the clock starts for determining compliance. - Simplify Part 2.1 by stating that any unauthorized individual is to be escorted. The revised language should be, "Require continuous escorted access of all individuals not authorized for unescorted physical access within each Physical Security Perimeter, except during CIP Exceptional Circumstances."
No
Yes
Yes
Yes
No
CIP-007-5-R1 - Part 1.1 requires clarification. The old language included "ports and services" whereas the new language includes "ports or services". The intent is only to track logical ports and related services. The following language should be used for the requirement, " For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges and related services where needed to handle dynamic ports. " - Part 4.1 replace the first sentence with "Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, per device capability, each of the following types of events." to better clarify that the requirement is limited per the capability of each of the devices in the Cyber System. - The language of Part 4.2.1 should be replaced with "detected cyber security event; and" since not all events are necessarily malicious. - Part 4.3 should be reworded as "Activate a response to a human detected event logging failure before the end of the next calendar day" to clarify that the clock needs to start upon a person picking up the notification, not when a system identifies the problem. - The wording in Part 4.5 should be changed to "Review a summarization or sampling as deemed appropriate by the Responsible Entity at a minimum every two weeks to identify undetected Cyber Security Incidents. " Rationale: It should be clear that the entity determines which logs should be reviewed or sampled to avoid confusion during audits.
CIP-007-5-R5 - Replace Part 5.1 with "Enforce authentication of all user account access, where technically feasible" to clarify that the access is electronic access and not physical access and to clarify that the requirement is to validate the accounts and not who is using the accounts (which is technically infeasible). Also, the applicability of the requirement should be limited High and Medium BES Cyber Systems with External Routable Connectivity. - Part 5.4 should be replaced with "Change known default passwords, where technically feasible, unless the default password is unique to the device or instance of the application, on Cyber Assets.". The addition of the word "known" is required to address system accounts that are not available to be changed without requiring a TFE. An example of such an account is the Windows "system" account. Also, the first measure should be changed to "Records of a procedure that passwords are changed when new devices are in production". Devices may be deployed, but not actively operating in production until their configuration is completed in the production environment. - The measures of Parts 5.5 and 5.6 should be modified for clarity of intent by replacing the second bullet with "Attestations that include a reference to the documented

procedures that were followed." The phrase “by individuals” is extraneous and the documented procedure will define the password parameters. The Application Guidelines for these requirements should also note that a single attestation may be used for both group of individuals performing password updates and groups of like assets that follow the same documented procedure. - Part 5.7, as written, is not recommended as it would create a potential vulnerability in the form of a Denial of Service attack. Limiting the language to "user accounts" eases this concern. The proposed language for this requirement is "Limit, where technically feasible, the number of unsuccessful authentication attempts for user accounts or generate alerts after a threshold of unsuccessful login attempts for all accounts."
Group
NESCOR/NESCO
Annabelle Lee
No
No
No
No
R3: Users of low impact BES cyber systems/assets also need basic cyber security training. Consider revising the training requirement to include basic cyber security training for all individuals. R4.2: The requirement only states criminal record checks and not other checks, such as random drug and alcohol testing. When people are drugged and/or intoxicated with alcohol, they may do things unknowingly, such as disclosing confidential information, losing confidential documentation and critical systems, and/or making improper judgments when running BES systems. Furthermore, drug and alcohol testing is reasonably commonplace in other industries and reasonable for both cyber security and safety. There should be consideration in this requirement to include drug and alcohol testing within the constraints of state laws and collective bargaining agreements. R4.4: It may be difficult to find contractors or vendors who have performed all the criteria listed in R4 (Personnel Risk Assessment Program). In many cases, these contractors and/or vendors, have been working for utilities for many years without any background or criminal check. What if the utility cannot get all that information? What if a utility finds something from the criminal record of a contractor who has been with them for several years? In these cases, what should the utility do? Additionally, must vendors be authorized to provide criminal background check information to the utility for their employees, which would require permission from the employee? Or can the vendor assert to the utility that it has obtained and verified this information in accordance with the CIPs? Current practice is to have the vendor and/or contractor attest to the fact that background checks (in accordance to the requirement) have been completed. Leveraging the TWIC program or creating a similiar program specific to the electric sector would lead to a consistent approach to 3rd party background screening and potentially reduce industry work effort on this activity.
R7.4 and 7.5: The requirements 7.4 and 7.5 allow time to remove physical and logical access privileges. Requirement 7.1 requires that termination procedures be initiated immediately. 7.4 and 7.5 allow a malicious individual time to initiate an attack.
No
No
There is no clear requirement that non-routable communications between two ESPs, such as between a substation and control center, be encrypted or have their integrity assured. Technical solutions exist to secure serial SCADA communications, both in the form of proprietary vendor products, as well as standards such as IEEE 1711 (developed from AGA12) and Secure DNP3. We suggest that all non-routable persistent communications links between ESPs be protected with strong encryption and integrity. Furthermore, the endpoint devices providing the encryption and authentication should be considered part of the ESPs and subject to all other CIP requirements for cyber assets belonging to an ESP. The lack of commercially available perimeter security solutions for non-routable protocols, pointed out in the Application Guidelines for CIP-005-5, further emphasizes the need for cryptographic protection of serial links. NERC's Consideration of Comments does not address this comment. This comment directly addresses point 86 in FERC 18 CFR Part 40 approving CIP v4, which states "...we support the elimination of the blanket exemption for non-routable connected cyber systems..." R1.3: We agree with identifying and documenting a business purpose for all inbound and outbound access from an EAP. However, this requirement should distinguish access through different

kinds of perimeters: 1. EAP allows traffic in/out over an encrypted link to/from another EAP owned/operated by the same entity; 2. EAP allows traffic in/out over a private but unencrypted link (eg. MPLS, point-to-point microwave) to/from another EAP owned/operated by the same entity; 3. EAP allows traffic in/out over an encrypted link to/from a system or EAP owned/operated by a different entity; 4. EAP allows traffic in/out over a private but unencrypted link to/from a system or EAP owned/operated by a different entity; 5. EAP allows traffic in/out over the public Internet. These cases involve differing degree of risk, with cases 1 and 2 being generally reasonable and justifiable; cases 3 and 4 utilities risky and avoidable with appropriate VPN technology, and case 5 being of far too high a risk to be acceptable, in our opinion, for any business purpose. A comment in the summary of changes for R1 states that "the non-routable protocol exclusion no longer exists". However, R1.1 and R1.2 all provide exclusions for non-routable protocols. We note that exclusions that existed in draft 1 R1.3 and R1.5 have been removed. There also remain exclusions in CIP 007 R1 and R4. We recommend removing all non-routable protocol exclusions, as the summary of changes claims. Despite the many changes in the language there is still too much ambiguity. "A method" for detecting communications is only also only half of the equation. There should be a method for detecting and addressing or mitigating detected anomalies. Perhaps a better phrasing would be: "Document and implement methods for detecting and addressing communications that have the characteristics of malicious or unexpected activity."
No
No
R1: As stated, "Define operational or procedural controls to restrict physical access." How is this consistent with the little or no security requirements for low impact systems? Also, as stated, low impact systems do not have to be uniquely identified. R3: NERC could consider adding a requirement to retest if the system fails.
No
No
No
No
No
R1: Table R1 is referred to as Ports & Services, but the controls are all about Ports, and there are no controls about services. NERC could consider either removing the reference to services or introduce a control to require an analysis of which services are running, and to disable or remove any services that are not necessary. Since Draft 1, the word “services has been added to the Requirements, but this does not address the point of this comment. Under the Guidelines and Technical Basis for Requirement R1, 1.1 the draft states “. . . therefore it is the intent that the control be on the device itself; blocking ports at the perimeter does not satisfy this requirement”. This seems to exclude the use of an intermediate device immediately preceding/inline with the device, thereby removing a valid security defense mechanism. Inline security mechanisms where no path around them exists enable security functionality to be placed in a manner to ensure they are engaged and also allow multiple solutions to be used where existing systems lack protection. An example would be a dedicated firewall and IPS system placed directly between a critical system and all connections, ensuring they are in the path of all traffic and allowing specialized security functions not available on some systems. A rewording of the quote above would add the option of providing non-bypassable security controls. “. . . therefore it is the intent that the control be on the device itself, or positioned inline in a non-bypassable manner; blocking ports at the perimeter does not satisfy this requirement”. R2: Patch management could also be considered for low impact systems. If the same operating system or application is used on low and medium/high impact BES systems, the patch should be applied to all the systems to mitigate the vulnerability. R2.1: This requirement states the need to identify the source or sources to be monitored for security patches, updates, etc. However, there is no mention of how frequent the responsible entity should be conducting this activity. It can be inferred from R2.2 that this activity must be conducted, at a minimum, every 29 days or less; however, as written, compliance is limited to identifying a source or sources and does not account for how often monitoring is to be conducted. If the intent is to have the responsible entity frequently monitor the identified sources so security patches, updates, etc. are discovered within 30 days of their release then the requirement should be more clear as to the monitoring expectations. As stated, "Update malicious

code protections within 30 calendar days of signature or pattern update availability (where the malicious code protections use signatures or patterns)." This requirement is specific to profiles. There are other techniques that address anomaly-based behavior analysis and heuristics based analysis/detection. NERC could consider revising the requirement to address other types of malicious code detection. R3.3: Previous draft stated 30 days between updates, this version increased it to 35 days. Again, 35 days is a lifetime when considering updating signatures/pattern files to malicious-code protection tools. Consider shortening this to a lesser period of time that is commensurate to the risk. The current requirement statement is long and confusing as well. Consider breaking it up into multiple sentence with clear requirement statements. R4: As stated, "Generate alerts for events that the Responsible Entity determines to necessitate a real-time alert." This is not specific to cyber security. Is that the intent? R4.2: There is still no requirement within the set of CIP standards 002-5 through 011-5 that make it clear that trained, knowledgeable and aware people are essential to making a security logging system fully functional. CIP-004-5 training requirements mention role-based training but without specific descriptions a responsible entity could have the alert analysis (and the R4.5 summary review) accomplished by an administrator who has no training or skills to perform such activity. Effective security log management requires aware and skilled personnel watching the log systems and output.
R5.2: As stated, "The CIP Senior Manager or delegate must authorize the use of administrator, shared, default, and other generic account types." How implement least privilege and other security controls if they are not defined in policy? This does not restrict the use of administrator, shared, etc. account types. These could be limited based on least privilege and need to know. As stated, "Identify individuals who have authorized access to shared accounts." Why only shared accounts? Consider identifying individuals with privileges – particularly those with access to administrator accounts. It is particularly important to identify administrators with privileges to modify the software itself. For example, I was unable to find a requirement in the standard that would discourage combined accounts for both operating and modifying software. CIP mitigations against malicious software currently appear limited to detection methods in CIP 010 - this would strengthen that position and is an auditable special case of least privilege in accordance with NIST 800-53 AC-6 control enhancement 2, which is required in the NIST baseline for moderate and high impact systems. It reads: "The organization requires that users of information system accounts, or roles, with access to [Assignment: organization-defined list of security functions or security-relevant information], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions." For CIP, at a minimum, "modification of software executing on medium or high impact BES systems" could be filled in the square brackets of this NIST requirement.
Group
FirstEnergy
Doug Hohlbaugh
Yes
Yes
Yes
Yes
Yes
No
No
We suggest modifying R2, part 2.7 to incorporate both training on “identification and response” and eliminating part 2.9. Our suggested re-write for R2, Part 2.7 is “Training content on identification, initial notification and response of a potential BES Cyber Security Incident in accordance with the entity’s incident response plan.” If this change is agreed to, conforming changes are also required to the Measure for part 2.7 to capture the inclusion of response.
(1) R6, parts 6.1, 6.2 6.3 and 6.4 we recommend replacing the word “designate” with “identify”. The term designate could cause confusion and need for interpretation as to who designated the authority to an individual(s) for authorizing access. This designation does not appear to be in the spirit of CIP-003-5 R5 (CIP Sr. Manager Delegate) nor should it be, therefore we recommend the change to “identify”. (2) In R6, part 6.5 related to the quarterly reviews of access provisions, the standard should permit a “find and fix” or “corrective action” approach for inadvertent access provisions that

are “found and fixed” based on two conditions – a) the error is corrected during the next quarterly review period occurring after initial access provisioning is granted and b) access to the area(s) provisioned was never used. Inadvertent access provisions can sometimes occur for employees having the same name (e.g. relatives Jr. vs. Sr.) and if identified and mitigated in a timely manner (next quarter) there should be no noncompliance if no actual reliability threat (no actual access) has occurred. As written, the standard promotes zero tolerance and is outside the spirit of these quarterly access reviews. (3) R7, part 7.1 - We do not support a need to revoke all access within 24-hours. This requirement is overly burdensome – especially in the case of trusted employee transfers who pose no real reliability threat. The 24-hour termination should be limited to “for cause” terminations of employment and additional flexibility built in for other situations (transfers, retirements, etc.) Consider and “equally and effective alternative” to the immediate terminations directed by FERC. If the concern from FERC is that the seven day period is too long then maybe some middle ground (3 business days) can be struck for the transfers and retirement scenarios. This requirement as written has the potential for numerous violations with questionable reliability benefit.
Yes
No
R2, Part 2.1, 2.2 and 2.3 require use of an Intermediate Device, encryption and multi-factor authentication, respectively. The requirements apply to Medium Impact BES Cyber Assets with no additional qualifiers; therefore it appears these would apply to all Medium BES Cyber Assets, even those with no external connectivity. These requirements should be limited to Medium BES Cyber Assets with External Routable Connectivity. Left unchanged will bring into scope a significant increase of cyber assets with no remote access capability for which the requirements are not feasible. Furthermore, the authentication for Medium BES Cyber Assets with dial-up connectivity is covered in CIP-005 R1, part 1.4 and CIP-005-5 R2, part 2.3, applicable to all Medium BES Cyber Assets, describes a need or multi-factor authentication and appears to be in conflict with R1 part 1.4.
No
Yes
Yes
FE’s concern with CIP-006-5 is requirement R1, part 1.4 which obligates a responsible entity to have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability). The requirement while well intended will likely lead to need for interpretation or guidance on the calculation of the 99.9% metric. For example, what is being measured the central monitoring station, the access panel controlling multiple points of entry at a substation, each door alarm or motion detector? Also, on what periodicity is the 99.9% stat based on? Is it an annualized calculation, intended to be a continuous running total 99.9% threshold? In summary, if kept, more guidance is required for how we measure and the period used for calculating the availability stat.
Yes
No
No
No
No
R2 (all parts), R3 (all parts), R4 part 4.1- these requirements deal with patch management, detecting and mitigating malicious code, logging and investigating cyber security incidents. The requirements apply to Medium Impact BES Cyber Assets with no additional qualifiers; therefore it appears these would apply to all Medium BES Cyber Assets, even those with no external connectivity. These requirements should be limited to Medium BES Cyber Assets with External Routable Connectivity. Left unchanged these will bring into scope a significant increase of cyber assets with no remote access capability for which the requirements are not feasible. Performing the requirements without remote diagnostics or service capability will require on-site visits to hundreds of remote substation locations to address a threat which can only be applied locally and having no ability to propagate to other BES locations. FE respectfully requests that the drafting team revise the applicability as requested above or provide the technical rationale for including cyber assets with no remote connectivity.
R5 part 5.1, 5.2 and 5.4 these requirements relate to enforcing access authentication, enabling

default or generic account types and revising default passwords. In regards to the Medium BES Cyber Asset applicability, FE believes it is important to limit to Medium BES Cyber Assets with external routable connectivity. Additionally, the applicability in question appears to be out of synch with CIP-004-5 R6, part 6.2 at least in regard to CIP-007-5 R5, 5.1. If the team believes dial-up should also be included, it would be an improvement over the existing draft text which includes cyber assets having no remote connectivity.
Group
MRO NSRF
WILL SMITH
Yes
No
No
Yes
Yes
Yes
No
: [R1] Though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] Each type of role-based training, Part 2.2-2.10, should be optional for some identified roles and required for others, and that distinction should be programmatically documented. That needs to be clearer in the structure of this requirement. If each of Part 2.2 through 2.10 were preceded with “Based on the role identified in Part R2.1…“ The way this is written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. More specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [R4]With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit.
[R7.2]: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need to straddle two jobs until a replacement is up to speed. [R7.3]: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. [R7.4]: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. : If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. [R7.5]: The "out" for extenuating operating

circumstances should be applied to all CIP 4 R7 requirements.
No
Yes
[R1.1] Proposed verbiage change for the applicability. [R1.1] “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. The requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken.
NONE
No
Yes
Yes
: [R1.2] Ensure applicability statements clarify that the associated EAC and Protected Cyber Assets are those associated with Medium Sites. [R1.4] –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are audit bait that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.5]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [R1.6] The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.7]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans.
Yes
No
No
No
No
Ensure the “zero defect” language in the VSLs is changed to be in alignment with EEI comments and the requirements, themselves. R1 – Consider exempting routable protocol on Medium Impact facilities for all CIP-007 R1 sub-requirements to maintain consistency. As currently drafted, some sub-requirements in R1 are exempt from routable protocol whereas others are not. Refer to the “Change Rationale” provided by the drafting team in R5.6 for the justification for this change. In all applicability columns, (CIP-007) where medium impact facilities are included, recommend including “with external routable connectivity”. [R1.1] Propose defining “network accessible” to clarify the requirements around the additional controls offered by firewalls and ports accessible only to the local host and whether those controls can be considered sufficient. Also recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. [R2] Although LES recognizes the revision as a good idea, we question whether including the monitoring of all installed cyber asset manufacturers is feasible. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. [R2.4] Recommend adding flexibility to change the plan without risking non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the planned and actual implementation.” [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. If a company were

to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. [R4.1], the Measure includes the phrase “is capable of detecting”. LES supports this phrase and believes it should be incorporated into the Requirement so companies are not required to replace equipment. Additionally, the “as a minimum” included in R4.1 seems to contradict the understanding of the Measure. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Ensure “High” is a qualifier for each of the systems identified in the applicability column. Proposed Verbiage to add clarity: “Document and implement a program to review a summarization or sampling of logged events, at a minimum, every two weeks, to identify un-alerted Cyber Security Incidents.” Rationale – with the documentation of a program, the entity can define the criteria for sampling and summaries without risking a finding of non-compliance when not meeting the interpretation-based expectation of an auditor.
[R5.1] Propose change to “within the capability of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change default passwords, unless the default password is unique to the device or instance of the application.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…”
Group
Southern Company Services, Inc.
Antonio Grayson
Yes
Yes
Yes
No
Yes
No
No
(1) Across all standards, the Measures need to be listed as “Examples” and be in a bulleted list “or” format. (2) Across each table in CIP-004-5, the table column header currently labeled “Applicable BES Cyber Systems and associated Cyber Assets” needs to be relabeled “Applicability” for consistency across all CIP standards. (3) Regarding CIP-004-5, R2, Southern suggests that it would be helpful if there was additional clarity around who must be trained, namely: “personnel with approved unescorted access or approved electronic access must have been trained.” (4) Regarding CIP-004-5, R3, Southern suggests removing the requirement of documentation as documentation is usually the measure. (5) Regarding CIP-004-5, R4, Southern believes that a timeline needs to be established. In 4.2, add “consecutive” before “six months or more”. Rationale: a support person, over a period of years, could accumulate six months in total. (6) Regarding CIP-004-5, R4, 4.2.1, 4.2.2 and 4.2.3 should be changed to a bulleted list. In 4.2.2 change the “and” to “or”. (7) Regarding CIP-004-5,

R4.1, this ‘bootstrap’ type requirement should be audited once per individual. As written, it would require the retention of this initial PRA for each individual forever. The requirement needs a maximum retention time per individual. (8) Regarding CIP-004-5, R4.1 needs a grandfathering provision (possibly in the implementation plan) for currently approved personnel. Rationale: Anyone with a documented background meeting the NERC CIP background requirements within the last seven years should be considered as already meeting the requirement. NERC CIP version 5 should not require that new background investigations be completed for those personnel who already have valid background documentation. (9) Regarding CIP-004-5, R4.3 and R4.4, the phrase “criteria or process” should be consistent between R4.3 and R4.4.
(1) Regarding CIP-004-5, R6, the rationale includes the important note that R6 does not apply to BES Cyber Systems that do not have user accounts defined. This needs to be included in the requirement itself rather than the rationale. (2) Regarding CIP-004-5, R6.1, change "designate" to "designate by name, role, or title" to clarify that entities can designate by title or role. (3) Regarding CIP-004-5, R6.2, “need to know” may be difficult to prove during an audit and represents a security guideline or rule of thumb that will be subject to varying interpretations. Southern suggests returning to language which demonstrates personnel have been “approved for access”. Southern believes that having approved approvers who grant all access is proof that :need to know" is considered for each request. (4) Regarding CIP-004-5, R6.3 implies that evidence of determination of need for performing work functions is needed for each physical access. Documentation of all roles and activities in advance is difficult for unescorted individuals. Southern suggests removing the words “that the Responsible Entity determines is necessary for performing assigned work functions” from the requirement. (5) Regarding CIP-004-5, R6.4, the SDT should consider whether this would include offsite storage of encrypted backup media or information being sent via postal service? If so, no entity can comply with the generic nature of this requirement. Southern suggests that the use of generic terms like “location” be struck and replaced throughout the standard as it applies to information protection with “designated repositories”. A similar change is required for R6.7. (6) Regarding CIP-004-5, R6.5, change “individuals provisioned” to “individuals currently provisioned” to eliminate from scope those who were provisioned but no longer need access. (7) Regarding CIP-004-5, R6.6, does "all user accounts and groups" on an EACM include all groups that may have nothing to do with CIP? If not, Southern suggests replacing "all" with “BES Cyber System” and clarifying intent within guidance and measures. (8) Regarding CIP-004-5, R6.6, in general, in terms of information management, “locations” needs to be replaced with “designated repositories” along with a requirement to list the repositories. The rationale for this change is that a location could be interpreted to be a car or an ipad, etc. For the purposes of information protection, designated repositories should be established. (9) Regarding CIP-004-5, R6.6, within the wording of the Measure, replace “Evidence may include, but is not limited to, documentation of the review including:” with “Example of the review of applicable cyber systems:”. (10) Regarding CIP-004-5, R7, 7.1, not all terminations are of equal risk (such as employee death). Southern strongly suggests restricting the tightest timeframes for deprovisioning to those terminations of higher risk, such as for cause terminations. In 7.2, the timeframe for completion of the activity should be based on the notification of re-assignment or transfer. In 7.3, the focus needs to be changed from "locations" to "designated repositories." In R7.4 – change "revoke" to either "remove or disable". In R7.5 – Southern recommends having the quarterly review be the cleanup of individual user accounts and not be considered a violation.
Yes
Yes
(1) Regarding CIP-005-5, R1, Southern suggests adding guidance to allow for implementation of IDS anywhere, internal or external to an ESP. Additionally, it’s not clear exactly how wireless networks are potentially impacted by CIP-005. (2) Regarding CIP-005-5, R1.1, the Measures should call for BES Cyber Systems to be documented rather than every component. (3) Regarding CIP-005-5, R1.4, if an entity does not use dialup, is a program required to authenticate dialup access? Consider using "if applicable" in the requirement. (4) Regarding CIP-005-5, R1.5 needs clarification on the path to be protected: internal, external, or both internal and external, and inbound and/or outbound.
(1) Regarding CIP-005-5, R2, clarification is needed that if "where technically feasible" occurs in the overall Requirement statement that it equally applies to all items in the subsequent table. (2) Regarding CIP-005-5, R2.2, the sentence in requirement should end after "Intermediate Device". The remainder of the sentence relates to overall rationale and not a requirement. (3) Regarding CIP-005-5, R2.3, clarification is needed that the two-factor authentication is to the Intermediate Device only.

No
Yes
Yes
(1) Regarding CIP-006-5, R1.2 and R1.3 as worded prevents escorted personnel from entering a PSP. Southern suggests deleting the word "unescorted" and clarifying that escorted personnel are authorized in this instance. (2) Regarding CIP-006-5, R1.3 needs clarification that multi-factor authentication, such as a physical badge and a biometric on the same access control system, is acceptable. (3) Regarding CIP-006-5, R1.4, measuring the 99.9% availability as included within the requirement causes more issues than it solves. Southern strongly suggests striking the 99.9% availability concept and language from all requirements and replacing it with the outage response requirements, including human observation, similar to the electronic monitoring requirement in CIP-007-5 R3. Additionally, Southern suggests noting that R3.2 implies that R1.4 is not necessarily 24x7 to allow for normal activities and unplanned outages. (4) Regarding CIP-006-5, Southern supports EEI's comments and strongly suggests returning to the monitoring of defined access points rather than the monitoring of perimeters. R1.4 needs to be deleted and R1.5 needs to be changed to “identified unauthorized access”. (5) Regarding CIP-006-5, R1.6 and R1.7 can be deleted if PACMS are added to the applicability column of R1.5. Therefore, Southern suggests removing R1.6 and R1.7 and putting PACMs in the applicability of R1.5.
Yes
Yes
Yes
Yes
No
(1) Regarding CIP-007-5, R1.1, Southern beleives that the measures for R1.1 do not satisfy the requirement. The Measures need to be reviewed to ensure the meet the requirement. The first measure should be deleted. (2) Regarding CIP-007-5, R2.2 and R2.3, the 30 calendar days needs to be changed to 35 calendar days to allow for coverage of monthly reports. Additionally, Southern believes there is an issue of double jeopardy between R2.2 and 2.3 that needs to be resolved. (3) Regarding CIP-007-5, R2.4, Southern believes that there is an issue of double jeopardy that needs to be resolved. Is the failure to implement in R2.4 also a failure of the "implement" in the overall Requirement? (4) Regarding CIP-007-5, R4, Southern suggests that the SDT consider referencing 800-137 within the appropriate guidance language. (5) Regarding CIP-007-5, R4.1, Southern suggests changing "at a minimum" with "per device capability". (6) Regarding CIP-007-5, R4.3, Southern suggests appending “after identification of the failure” to clarify when the response period begins.
(1) Regarding CIP-007-5, R5.2, Southern questions the benefit of a senior manager approving that generic accounts exist when we already have to authorize individuals to use those accounts. This is a too low level task for a senior manager. To address this issue and to avoid unnecessary duplication, Southern strongly suggests removing R5.2 as the security intent is achieved through R5.3. (2) Regarding CIP-007-5, R5.3, the point concerning lost or inappropriate passwords in the change rationale is an important point and Southern suggests moving it to the guidance. (3) Regarding CIP-007-5, R5.5, Southern suggests that the "attestation" in the measures be changed to "documentation". (4) Regarding CIP-007-5, R5.7, Southern strongly suggests deleting the requirement as it is not in Order 706 and it provides opportunity for denial of service attacks. Locking out accounts may be viable in the IT systems, but may introduce more risk in BES Cyber Systems if critical accounts can be locked out by simply trying known invalid credentials. If the requirement stays, we suggest moving ‘where technically feasible’ to the beginning of the requirement so it is clear that a TFE is available for both options.
Group
Western Area Power Administration
Brandy A. Dunn
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
No
No
No
R1.4 and R1.6 “require 99.9% availability”; a definition of this requirement is need. Does this include maintenance and testing time? Upgrade time? Also, what are acceptable monitoring methods to meet the “controls that monitor” intent?
No
No
Yes
No
Yes
CAN-0019 is in development to answer the question, “What is the acceptable time to install a software patch before a TFE is required?” CIP-007-5 R2 states that a remediation plan must be developed within 30 days, but does not answer the question. Please identify an acceptable interval for completion of the remediation plan. Is one year too long? Can a remediation plan state that implementation will start after 6 years?
Individual
Brian S. Millard
Tennessee Valley Authority
Yes
Yes
Yes
Yes
Yes
Yes
Yes
CIP-004-5 R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based infers that training should be based on access permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Remove R2.10, What is the intent of this requirement? There is no additional value in this requirement as it is already covered in 2.2 through 2.9. CIP-004-5 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based infers that training should be based on access permissions or that access should be role based. CIP-004-05 R 2.8 - Remove the requirement for training content for recovery plans for BES Cyber Systems. Rationale to apply this training to all personnel who have access to BES Cyber Systems is flawed. A small subset of skilled individuals would be responsible for executing recovery plans not the entire CIP population. R3.1 - Requirement should not include documentation, this is a measure. R4.1 - Time period for retention is not defined. Need to include provision for grandfathering older standard requirements. R4.2 - Include the word “consecutive” prior to six months. Make a bulleted list to represent and “or” list. CIP-004-5 R4 - The ability to verify criminal history for employees who haven’t resided in the US for more than a few years may cause employment issues for employees.

Rational R6 - User Accounts are not defined or called out in actual standard. R6.1 - Designate one or more individuals by names or roles. R6.2 - Remove “the Responsible Entity determines”, the function of the authorizer in R6.1 is to ensure need. R6.4 - Use the word “designated repository” instead of “location”. With location, this could be an iPad. R6.5 - Add “currently” between” individuals provisioned”. Reword to match current quarterly review and comparison of who needs access versus who has access. R6.6 - Replace “all” with BES cyber systems. Change number list in measures to bulleted list to represent an “or” list. R7.7 - Use the word “designated repository” instead of “location”. R7.1 - Employee death should be classified differently than termination. Possibly use no longer requiring access vs. termination. 7.1 should be reserved for someone who is a risk. R7.2 - Insert “notification of” prior to reassignments. Allow for one barrier approach or effectively remove. R7.3 - Use the word “designated repository” instead of “location”.
Yes
Yes
CIP-005 R1.7 - Language in this standard is conflicting and arbitrary. The measures section of R1.7 references a specific term with Intrusion Detection Systems. There are numerous types of technology which can identify malicious traffic. Remove the measures language or make it technology agnostic. The expansion of the requirements and assets covered under R1 will require the addition of personnel and systems that are not currently in place today. The requirement for 1.5 is “Have a method for detecting malicious communications.” The intention of this standard is unclear. It is not clear what “malicious communications” is, nor is it clear what an acceptable method is. Is an IP address ping sweep “malicious communication”? If so, then could you just have a firewall send alerts when there are dropped packets? The Measures section mentions intrusion detection systems but does not discuss what minimum configuration requirements are needed. As written, it appears that a poorly implemented IDS would meet the word of the standard. For example, it sounds like one would only need to provide a configuration file of an IDS and documentation of where it is located, but not have to provide evidence that it is continuously working or that its configuration is appropriate. R1.1 Measures - Delete “uniquely identifiable”, should be with all BES in ESP not at component level. R1.4 - Include applicable, you do not need to have a program if you don’t need or use dial up connectivity.
CIP-005 R2.2 - The requirement does not reference specific types or standards for acceptable levels of encryption. This will lead to regions interpreting this differently and impact the ability of the business to meet this requirement. Consider referencing NIST approved encryption methodologies (i.e. NIST SP800-77 or NIST SP800-111). R2.2 - End the sentence after intermediate device. Balance is commentary. R2.3 - Clarify that this is to the intermediate device only.
No
Yes
Yes
R1.2 - As worded, this prevents an escorted person from entering the PSP. R1.3 - Modify controls wording to be multi-factor authentication. As worded this prevents an escorted person from entering the PSP. R1.4 Meeting the 99.9% is not possible. How do we measure and what is the threshold? Suggest rewording to be like CIP-007 R 4.3. Need to include provisions for mitigation with personnel. Consider making applicable to only High impacts and lesser degree for Medium impacts. Bounds should be set around monitoring. Consider limiting to physical access points. R1.5- Replace “circumvention” with “access”.
Yes
Yes
Yes
Yes
No
CIP-007 R2.3 - Due to the sheer number and volume of patches that are issued for both information technology and operational technology this requirement becomes overly burdensome. CIP-007 R 4.2 - The term “necessitate a real-time alert” is introduced to the standard. Is there a threshold for what is deemed a real-time alert? The term is unnecessarily vague and will lead to regional interpretation issues. Suggest striking the term. CIP-007 R 4.5 - This requirement should be reworded to address manual review at a minimum every two weeks for manual logging activity and should be excluded where automated monitoring programs are in place (i.e. Managed Security Service

Provider).Additional resources would be required for managing and monitoring additional devices that would be covered in the revised requirement. R2 - No requirement to maintain a system that is patchable thereby, rewarding obsolescence. Understandably, a grace period for upgrading to a patchable should be allowed, but to never require upgrading is too liberal and a security risk. R2.2 - Change 30 days to 35 days in order to allow monthly evaluations. R3.3 - Update cycle too aggressive. It should match patching requirements for practical testing, scheduling, and outage installation. Language will force online updates with undue risk. R4.1 - Replace “minimum” with “per device capability”. R4.3 - Change detected to indicate human detected. Add “after notification” to the end of “next calendar day”. R4.4 - Remove Security Event Logs and replace with previous 4.1 logs.
R5.2 - Recommend deleting requirement. The CIP Senior Manager approval of shared accounts adds administrative burden without cyber security benefits. R5.7 - Recommend deleting requirement. This could result in control system lockout and have a negative impact on reliability.
Group
Edison Electric Institute
David Batz
(1.) Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources. (2.) Other applicability concerns - There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. The primary concern is that the applicability of 'Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity' is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. In some instances the inconsistency can be cleared up by changing the applicability from 'Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity' to 'Medium Impact BES Cyber System with External Routable Connectivity.' There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. As one example, the applicability of CIP-004 for physical access control systems exceeds that of CIP-006. To increase consistency within the standards, references to dial-up connectivity has been removed where alignment within CIP-006 is necessary. Dial-Up access is only referenced within CIP-004 applicability columns (within the Standard). (3.) Suggest limiting applicability to the access control of BES Cyber Systems. There is confusion where electronic and physical access control systems fall within the requirements, whether the applicability is limited to access control of BES Cyber Systems. (4.) With respect to R5.1, there is some concern regarding the current triggers of 'being granted' access and authorizing access. There was some discussion of replacing 'being granted' with 'provisioning,' but no clear consensus was identified. (5.) R1.1 - Requirements a. Propose changing the phrase 'ongoing reinforcement of cyber security practices,' to 'ongoing reinforcement of security practices.' By dropping 'cyber,' a more general security awareness program can be implemented, addressing cyber and physical awareness topics. b. Insert 'unescorted' into 'authorized unescorted electronic' references. This allows entities to focus on unauthorized access rather while allowing for vendor support services. (6.) R2.1 - Requirements, Rewording a. Original - Identification of each role and training required for each role. b. Proposed - Identification of training content appropriate for individuals and their responsibilities c. Rationale - The rewording allows for increased flexibility in an entities training approach, while ensuring topics adequately cover CIP training requirements. (7.) R2.2 - Requirements, Rewording a. Original - Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems. b. Proposed - Training content on the cyber security policies protecting applicable cyber assets. c. Rationale - This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). (8.) R2.3 - Requirements, Rewording a. Original - Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems. b. Proposed Training content on the physical access

controls protecting applicable cyber assets. c. Rationale - This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). (9.) R3.1 - change reference from 'BES Cyber Systems' to 'applicable cyber assets' to ensure training adequately covers relevant and applicable cyber assets. (10.) R4.1 - Requirements, Rewording a. Original - An initial personnel risk assessment ('PRA') that includes identify verification. b. Proposed - Program content on an initial personnel risk assessment that includes identity verification. c. Rationale - This requirement should address the contents of a supporting program rather than individual artifacts of evidence. (11.) R4.2 - Requirements, Rewording a. Original - Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: b. Proposed - Seven year criminal history records check including current residence, regardless of duration, and covering all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more: c. Rationale - Two changes have been made. 'At least' was dropped in front of 'all' as it was redundant with 'at least all.' Also, 'consecutive' was added in the middle of 'six months' to provide greater clarity in terms of what the criteria is. (12.) R5.1 - Requirements, Rewording a. Original - Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. b. Proposed - Have a personnel risk assessment as specified in CIP-004-5, Requirement R4 prior to gaining authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Subsequent authorizations, within the life-time of PRA events, do not require repeating the background check. c. Rationale - while not perfect, it was determined that 'gaining' would be better terminology than 'granting.' The additional language regarding not repeating this requirement provides clarity that this process is to be conducted once for any/all authorized access and is not subject to additional PRAs as additional access requirements are identified. (13.) R5.1 - Measures, Rewording (First bullet) a. Original - Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or b. Proposed - Records showing that personnel risk assessments were performed before authorized unescorted electronic or authorized unescorted physical access was gained. c. Rationale - There is repetition of 'authorized' within this measure which is confusing. By replacing the last word with provisioned, the event is better captured to ensure compliance with the PRA requirement. (14.) R5.2 - Measures, Rewording a. Original - Evidence may include, but is not limited to, current and previous personnel risk assessment records. b. Proposed - Evidence may include, but is not limited to, current personnel risk assessment records. c. Rationale - Given the 7 year cycle, ensuring that the current records are in place should satisfy this requirement. Addition of previous PRA records only adds to the archival length to a period of (up to) 14 years without any benefit to security.

(15.) R6.1 a. Applicability should remove references to dial-up connectivity b. Measure should add 'unescorted' in front of electronic access. c. Rationale - this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into 'authorized electronic access' category. (16.) R6.2 Requirement Rewording a. Original - The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed - The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate. c. Rational - assessing the appropriateness of access permissions is more effective then assessing 'necessary.' (17.) R6.3 Requirement Rewording a. Applicability should remove references to dial-up connectivity b. Original - The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. c. Proposed - The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances. d. Rationale - Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. (18.) R6.6 Requirement Rewording a. Original - For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. b. Proposed - For electronic access, verify at least once each calendar year, or not to exceed 15 calendar

months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. c. Rationale - The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating 'all,' identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. 'correct,' allows for assessing the privileges. (19.) R6.6 Measures - This should be a bulleted list to support an 'or' assessment of the evidence. (20.) R6.7 Measures - The numbered list should be a bulleted list to support an 'or' assessment of the evidence. a. Last bullet - Rewrite i. Original - Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed - Evidence showing a verification of the authorization and any permissions were confirmed. iii. Rationale - The edits provide a greater focus on the root concerns to address the Requirement. (21.) R7.1 - Requirement Rewrite a. Original - For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. b. Proposed - For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. c. Rationale - By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. (22.) R7.1 - Measure should show a bulleted list to reflect the 'or' approach to supporting evidence. (23.) R7.2 - Requirements Rewrite a. Original - For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. b. Rewrite - For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary. c. Rationale - The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. (24.) R7.2 - Measure should show a bulleted list to reflect the 'or' approach to supporting evidence. (25.) R7.5 - Frame the requirement against BES Cyber System shared accounts to provide alignment with BES Cyber Systems.
(1.) While dial-up connectivity requirements are proposed to be moved to CIP-007-5, R5.1, there should be a definition identifying what constitutes 'dial-up.' EEI membership discussed varying interpretations that indicate a clearer definition would help identifying the applicable cyber assets. Proposed definition: Dial-Up connectivity - Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). (2.) Definition - Intermediate Device a. Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. b. Rationale - This will ensure applicable Intermediate Devices are not 'disqualified' from operating as such should they have an interface which is an electronic access point into the ESP. (3.) Introduction - 4.2.2: This should reference CIP-005-5 (rather than CIP-002-5). (4.) R1.1: Applicability a. Add Associated Protected Cyber Assets with External Routable Connectivity b. Rationale - This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. (5.) R1.2 Applicability a. Add Associated Protected Cyber Assets with External Routable Connectivity b. Rationale - This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. (6.) R1.4 a. This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. b. Propose adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. c. Rationale - This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. (7.) R1.5 Measures - there should be bullets (rather than numbers) identifying 'or' instances.
(8.) R2.1, 2.2, 2.3 Requirements - Proposed Change a. Original - Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. b. Proposed - Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device. c. Rationale - The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept. (9.) R2.3:

Requirements - Move examples cited into the measures for the three factors cited, leaving the requirement with the description of the factor. The measures would frame examples appropriate to each factor. (10.) R2.4: Clarification as to where the authentication needs to take place. Can the multi-factor authentication be done at the intermediate device or does it need to be done at the access point to the ESP.
(1.) R1.4 is seen as a deal breaker and should be considered for removal. Monitoring 24*7*365 with a 99.9% uptime would require extensive resources to satisfy the supporting documentation. Comment to revise is contained in the comment on R1.5. R3.2 justifies that this level of monitoring is not required. (2.) Focusing on unauthorized circumvention of physical access control could be interpreted as monitoring for perimeter breaches outside of the current physical access points. This could lead to exhaustive monitoring tools which may still allow for unmonitored locations that result in a violation of this requirement. (3.) The category of 'locally mounted hardware or devices at the Physical Security Perimeter(s)' requires additional detail. This originates within the PSP definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. By defining something by what it is not, there is a risk that it may include a number of devices beyond the intended PSP devices. (4.) Introduction - Section 4.2.3: By citing 'All BES Facilities' there may be a perceived exclusion of ISOs from applicability. This should reference the ISO role as also being subject to CIP-006-5. (5.) The applicability within this Standard was a topic of extensive discussion. a. Within 1.1-1.8, it is unclear whether 1.1 is intended to apply to devices not cited within 1.2- 8. Per the first draft, 1.1 was intended to capture devices not subject to subsequent standards. If this is the approach for draft 2, the applicability should include (only) dial-up accessible and externally routable devices. Associated Electronic Access Control devices should also be included within R1.1 applicability. b. In any event, this may be an instance in which diagrams or other graphical aides may benefit the understanding of what devices are subject to what requirements via a series of pictures. (6.) The concept of 'two or more different physical access controls' needs additional supporting documentation, including appropriate strategies to satisfy this requirement. Can a common server that satisfies authentication request from multiple access controls satisfy this requirement' Is the intent to require two 'keys' or authentication factors' It is also unclear how two factor authentication would fit into satisfying this requirement. (7.) Introduction 4.2.4: This should reference CIP-006-5 (rather than CIP-002-5). (8.) R1.5 a. Requirement: This includes content similar to R1.4, which has been proposed for removal. The concept of 'unauthorized circumvention of a physical access control' may require resources and technology which may still be inadequate to identify any/all instances of circumvention. Changing 'unauthorized circumvention' to 'unauthorized access' may better frame this requirement, but may not satisfy the root concern intended by the SDT. b. Measures - there should be bullets (rather than numbers) identifying 'or' instances. (9.) R1.7 Requirements & Measures - Change a. Original - Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. b. Proposed - Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System within 15 minutes of the detected unauthorized physical access. (10.) R2.1 - Requirements a. Original - Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances. b. Proposed - Require continuous escorted access of individuals not authorized for unescorted physical access. c. Rationale - The additional words did not provide any greater clarity. (11.) R3.2 a. Applicability - Remove 'Locally mounted hardware or devices at the physical security perimeter associated with:' Rationale - documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. b. Requirement - Change i. Original - Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. ii. Propose - Document outages for physical access control systems and retain the outage records for at least 12 calendar months. iii. Rationale - By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved. (12.) VSL - R1/High: The second paragraph on page 23 should read 'The Responsible Entity does not have controls' (13.) VSL - R1/Medium: Remove 'or external dial-up connectivity. (1.2)' from the end of the second paragraph. (14.) VSL - R2 Moderate: Remove 'on a daily basis,' from the 1st paragraph on page 25. (15.) Application Guidelines a. Page 28 - Remove 'Methods to monitor physical access include:' section as it relates to R1.4, which has been proposed for removal. b. Page 29, second paragraph - Remove. The applicability of the 96 square inch opening

provides no benefit to applicability.
(1.) R2, all sub-requirements Applicable BES Cyber Systems and associated Cyber Assets: Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routable Connectivity'. Rationale: For non-externally routable or dialup systems this will create a large amount of document requirements without adding much security. (2.) R1.1 a. Applicable BES Cyber Systems and associated Cyber Assets: Clarify how 'Associated Protected Cyber Assets' is a modifier to the 'High Impact BEST Cyber Systems' and 'Medium Impact BES Cyber Systems with External Routable Connectivity' rather than an independent set of assets. One option is to add 'and Associated Protected Cyber Assets' to each of the High and Medium categories in this requirement. b. Requirements i. Does the 'where technically feasible' language imply that TFEs are required when it is not technically feasible' ii. There was discussion about how 'needed' should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. (3.) R1.2 a. Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. b. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. (4.) R2.1 Requirements: Original - 'A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets.' Proposed - 'A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets.' (5.) R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency (6.) Requirement 3 & 4, all sub-requirements a. Associated Protected Cyber Assets i. Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. ii. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. (7.) User vs. System password: A long discussion ensued that there is no clear delineation between system passwords and user passwords. Does a user password have an identity associated with it' What about systems that use system ids/passwords, do those qualify as user or system passwords' Clarification of this issue would be helpful. (8.) R4.1 a. Add the term 'where technically feasible' to the requirement language b. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. (9.) R4.2.1 a. Change 'detected malicious activity' to 'detected cyber security event' b. Rationale: not all security events are malicious (10.) R4.3 a. Requirement i. Change 'Activate a response to detected event' to 'Activate a response to human-detected event' ii. Rationale: the requirements do not distinguish between the detection of an event by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. b. Requirement: Change 'next calendar day' to 'next business day' to accommodate off-hour staff coverage. c. Measures: Change 'attestation' to 'documentation' for clarity. (11.) R4.5 a. Applicability i. Consolidate 'High Impact BES Cyber Systems' and 'Associated Protected Cyber Assets', by changing the wording to 'High Impact BES Cyber Systems with Associated Protected Cyber Assets' ii. Rationale: Clarifies that the logging reviews do not apply at the asset level. b. Requirement i. Change the wording to 'Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum' ii. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
(12.) R5.1 a. Applicability i. Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routability or dial -up' ii. Rationale: Consistency with CIP-004 R6.2 (13.) R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 (14.) R5.3 Delete requirement, and move rationale to CIP-004 R6. Rationale: Covered by CIP-004 R6. (15.) R5.4 a. Applicability i. Change 'Medium Impact BES Cyber Systems' to 'Medium Impact BES Cyber Systems with External Routability or dial -up' ii. Rationale: Consistency with CIP-004 R6.2 b. Requirement i. Change the wording from 'Change default passwords' to 'Change known default passwords' ii. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. c. Measures i. Remove the language from the first bullet 'when new devices are deployed' ii. Rationale: Time frames are covered elsewhere in the Standards (16.) R5.5 Measures a. Change the second bullet to 'Documentation of procedural controls' b. Rationale: Procedural controls for changing passwords are covered elsewhere (17.) R5.6 a. Requirement i. Add the language 'within the capabilities of the device or operational requirements' to the beginning of the requirement. ii. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. b. Measures i. Change the

second bullet to 'Documentation of procedural controls' ii. Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
Andrew Z. Pusztai
American Transmission Company, LLC
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
ATC endorses the comments that EEI formulated as consensus comments and submitted for entire Comment Form B.
Individual
Ralph Meyer
The Empire District Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
1. Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources. 2. Other applicability concerns – the applicability of CIP-004 for physical access control systems exceeds that of CIP-006. To increase consistency within the standards, references to dial-up connectivity has been removed where alignment within CIP-006 is necessary. Dial-Up access is only referenced within CIP-004 applicability columns (within the Standard). 3. There is also confusion where electronic and physical access control systems fall within the requirements, whether the applicability is limited to access control of BES Cyber Systems. 4. 6. R2.1 – Requirements, Rewording a. Original – Identification of each role and training required for each role. b. Proposed – Identification of training content appropriate for individuals and their responsibilities c. Rationale – The rewording allows for increased flexibility in an entities training approach, while ensuring topics adequately cover CIP training requirements.
15. R6.1 a. Applicability should remove references to dial-up connectivity b. Measure should add ‘unescorted’ in front of electronic access. c. Rationale – this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into ‘authorized electronic access’ category. 16. R6.2 Requirement Rewording a. Original – The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed – The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate for the individual role and responsibility. c. Rational – assessing the appropriateness of access permissions is more effective

then assessing 'necessary.' 17. R6.3 Requirement Rewording a. Original – The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. b. Proposed – The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. c. Rationale – Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. 18. R6.6 Requirement Rewording a. Original – For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. b. Proposed – For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. c. Rationale – The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating "all," identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. "correct," allows for assessing the privileges. 19. R6.6 Measures – This should be a bulleted list to support an "or" assessment of the evidence. 20. R6.7 Measures – The numbered list should be a bulleted list to support an "or" assessment of the evidence. a. Last bullet – Rewrite i. Original – Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed – Evidence showing a verification of the authorization and any permissions were confirmed. iii. Rationale – The edits provide a greater focus on the root concerns to address the Requirement. 21. R7.1 – Requirement Rewrite a. Original – For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. b. Proposed – For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. c. Rationale – By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. 22. R7.1 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence. 23. R7.2 – Requirements Rewrite a. Original – For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. b. Rewrite – For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination. c. Rationale – The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. 24. R7.2 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence. 25. R7.5 – Frame the requirement against BES Cyber System shared accounts to provide alignment with BES Cyber Systems.
Yes
Yes
1. While dial-up connectivity requirements are proposed to be moved to CIP-007-5, R5.1, there should be a definition identifying what constitutes "dial-up." EEI membership discussed varying interpretations that indicate a clearer definition would help identifying the applicable cyber assets. Proposed definition: Dial-Up connectivity – Connectivity to BES Cyber Assets (or associated Protected Cyber Assets) which is publically accessible using the Publically Switched Telephone Network (PSTN). 2. Definition – Intermediate Device a. Modify the definition to allow for Intermediate Devices to terminate on an Electronic Access Point or to be external to the ESP. b. Rationale – This will ensure applicable Intermediate Devices are not 'disqualified' from operating as such should they have an interface which is an electronic access point into the ESP.
8. R2.2 Requirements – Proposed Change a. Original – Utilize encryption for all Interactive Remote

Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. b. Proposed – Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. c. Rationale – The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept.
Yes
Yes
Yes
11. R3.2 a. Applicability – Remove "Locally mounted hardware or devices at the physical security perimeter associated with:" Rationale – documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. b. Requirement – Change i. Original – Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. ii. Propose – Document outages for physical access control systems and retain the outage records for at least 12 calendar months. iii. Rationale – By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved.
Yes
Yes
Yes
No
Yes
1. R2, all sub-requirements Applicable BES Cyber Systems and associated Cyber Assets: Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity". Rationale: For non-externally routable or dialup systems this will create a large amount of document requirements without adding much security. 2. R1.1 a. Applicable BES Cyber Systems and associated Cyber Assets: Clarify how "Associated Protected Cyber Assets" is a modifier to the "High Impact BEST Cyber Systems" and "Medium Impact BES Cyber Systems with External Routable Connectivity" rather than an independent set of assets. One option is to add "and Associated Protected Cyber Assets" to each of the High and Medium categories in this requirement. b. Requirements i. Does the "where technically feasible" language imply that TFEs are required when it is not technically feasible? ii. There was discussion about how "needed" should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. 3. R1.2 a. Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. b. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. 4. R2.1 Requirements: Original – "A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets." Proposed - "A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." 5. R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency 6. Requirement 3 & 4, all sub-requirements a. Associated Protected Cyber Assets i. Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. ii. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. 7. User vs. System password: A long discussion ensued that there is no clear delineation between system passwords and user passwords. Does a user password have an identity associated with it? What about systems that use system ids/passwords, do those qualify as user or system passwords? Clarification of this issue would be helpful. 8. R4.1 a. Add the term "where technically feasible" to the requirement language b. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. 9. R4.2.1 a. Change "detected malicious activity" to "detected cyber security event" b. Rationale: not all security events are malicious 10. R4.3 a. Requirement i. Change "Activate a response to detected event…" to "Activate a response to human-detected event…" ii. Rationale: the requirements do not distinguish between the detection of an event

by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. b. Requirement: Change “next calendar day” to “next business day” to accommodate off-hour staff coverage. c. Measures: Change “attestation” to “documentation” for clarity. 11. R4.4 a. Applicability i. Remove the three “Associated…” systems/assets from the applicability section ii. Rationale: Confusing because the requirement states “BES Cyber System” which does not include these associated systems. b. Measures: Change the numbers to bullets for document consistency 12. R4.5 a. Applicability i. Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets” ii. Rationale: Clarifies that the logging reviews do not apply at the asset level. b. Applicability i. Remove “Associated Physical Access Control Systems” and “Associated Electronic Access Control or Monitoring Systems” ii. Rationale: c. Requirement i. Change the wording to “Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…” ii. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
13. R5.1 a. Applicability i. Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” ii. Rationale: Consistency with CIP-004 R6.2 14. R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 15. R5.3 Delete requirement, and move rationale to CIP-004 R6. Rationale: Covered by CIP-004 R6. 16. R5.4 a. Applicability i. Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” ii. Rationale: Consistency with CIP-004 R6.2 b. Requirement i. Change the wording from “Change default passwords…” to “Change known default passwords…” ii. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. c. Measures i. Remove the language from the first bullet “…when new devices are deployed” ii. Rationale: Time frames are covered elsewhere in the Standards 17. R5.5 Measures a. Change the second bullet to “Documentation of procedural controls” b. Rationale: Procedural controls for changing passwords are covered elsewhere 18. R5.6 a. Requirement i. Add the language “unless it impacts operation of the BES” to the end of the requirement. ii. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. b. Measures i. Change the second bullet to “Documentation of procedural controls” ii. Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
Kirit Shah
Ameren
Yes
No
No
No
Yes
No
No
(1) General comments – We suggest that anywhere that the words "authorized electronic" is used in CIP-004 should be replaced with "unescorted authorized electronic"; this language change would allow an entity to have escorted electronic access. Also, the words "but is not limited to" needs to be removed from the measures to clarify what documentation is needed for compliance. (2) R1.1 – Remove the word "cyber" in front of the words "security practices" in the requirement. This will allow and entity to broaden its security awareness program to include physical or other types of security practices outside of just cyber. (3) R2.1 – Change the language in the requirement to "Identification of appropriate training required for individual based on their responsibilities". This wording would allow more flexibility in the type of training each individual would receive and not require an entity to create roles. (4) R2.2 – Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (5) R2.3 – (a) Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (b) In the Applicability section this training should only be required for "Associated Physical Access Control Systems for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity".

This language change would limit only individuals that have access to the Physical Access Control Systems to take this training. (6) R2.4 – (a) Add the word "Applicable" before the word "Entity" to require training for only the applicable BES Cyber Systems and not for all BES Cyber Systems in the requirement. (b) In the Applicability section this training should only be required for "Associated Electronic Access Control or Monitoring Systems for High Impact BES Cyber Systems and Medium Impact BES Cyber Systems with External Routable Connectivity". This language change would limit only individuals that have access to the Electronic Access Control or Monitoring Systems to take this training. (7) R2.8 – Currently Recovery Plan information is considered confidential. Labeling specific information to be held in a training program should be removed, and information should be at the discretion of the entity to put into their program. (8) R2.10 – Remove the words "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" from the Applicability section. This language change would remove personnel that have access to "Associated Physical Access Control Systems and Associated Electronic Access Control or Monitoring Systems" from taking training on "BES Cyber System's electronic interconnectivity and interoperability with other Cyber Assets". (9) R3 – "Role Based cyber security training is very vague. How many roles does the SDT intend for entities to define. If there are specific roles to cover, they should be included in the standard. (10) R3.1 and R3.2 – Add the word "Applicable" in front of the words "training specified" and change "BES Cyber Systems" to "applicable cyber assets" in the requirement. These word changes will help clarify what type of training is needed to meet this requirement. (11) R4.1 – Add the words "A documented personnel risk assessment program requiring" at the beginning of the requirements. This word change will help clarify that a program needs to be established for personnel risk assessments. (12) R4.2 – (a) Remove the words "at least" and add the words "consecutive" in front of the words "six months" in the requirement. These word changes help clarify this requirement. (b) Remove items 4.2.1, 4.2.2, and 4.2.3. The requirements of the PRA and action based on the results should be the discretion of the entity. (13) R4.3 – Remove the words "or criteria" in the requirement and the words "or criteria identified" in the measures. This wording helps clarify that you need a process to evaluate personnel risk assessments. (14) R5.2 – Add the word "one" in front of the word "previous" in the measures. This wording helps an entity to only have to have one previous personnel risk assessment for documentation purposes.

(1) General comments – (a) For all of R6 remove the words "dial-up connectivity" in the applicability. This change matches this requirement with other dial-up connectivity requirements. (b) The words "but is not limited to" needs to be removed from the measures to clarify what documentation is needed for compliance. (2) R6.1 – (a) Remove the words "dial-up connectivity" in the applicability. (b) Add the words "to a Physical Security Perimeter" after the words "unescorted physical access" in the applicability. These changes match this requirement with other dial-up connectivity and unescorted physical access requirements. (3) R6.2 – Remove the words "for performing assigned work functions" after the word necessary in the requirement. This change helps clarify this requirement. (4) R6.3 – Change the wording of the requirement to "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is necessary, except for CIP Exceptional Circumstances". This change matches this requirement with other unescorted physical access requirements. (5) R6.4 – Remove the words "are necessary for performing assigned work functions" and replace with "are necessary" in the requirements. This change helps clarify this requirement. (6) R6.5 – Add the words "to BES Cyber Systems" after the words "physical access" in the requirements. This clarifies what type of access needs to be verified each quarter. (7) R6.6 – Replace the word "all" with "BES Cyber Systems" and replace the word "correct" with "necessary" in the requirements. This change helps clarify this requirement. (8) R7.1 – (a) Replace the words "upon the effective date" with "within 24 hours" and replace "24 hours" with "7 business days" in the requirement. This will give an entity a reasonable and achievable time to remove access. Allow seven days. (b) Change the numbers to bullets in the measures to reflect the list approach. (9) R7.2 – (a) Replace the words "by the end of the next calendar day" with "within 7 business days" in the requirement. This helps match the access removal time to the security risk of the access being removed. For a transfer an employee who is still an employee of the company in good standing should not require an end of the next calendar day removal, but should be given 7 days (b) Change the numbers to bullets in the measures to reflect the list approach. (10) R7.3 – Replace the words "by the end of the next calendar day" with "within 7 days" in the requirement. This helps match the access removal time to the security risk of the access being removed. For a removal of access to only information, this type of access should not be required to be removed by the end of the next calendar day.

Yes
No
(1) R1.1 - Add the words "Associated Protected Cyber Assets with External Routable Connectivity" to the applicability in order to align the applicability with the requirement. (2) R1.2 - Add the words "with External Routable Connectivity" after the words "Associated Protected Cyber Assets" to the applicability in order to align the applicability with the requirement. (3) R1.5 – Remove the word "and" and make the numbers into bullets in the measure to help clarify the instance of "or" instead of "and".
(1) R2.1 and R2.2 – (a) The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "Medium Impact BES Cyber Systems". Otherwise, encryption would be required for all Interactive Remote access to substations (which will fall under these requirements) which would be difficult to implement if even possible. (b) Add the word "Routable" in front of the words "Interactive Remote Access" to clarify that the type of remote access that is allowed for this requirement. (2) R2.3 – Move the examples in the requirement to the measures section to give examples of what is appropriate for multi-factor authentication.
No
Yes
Yes
(1) General Comments – (a) CIP-006 is very confusing and there needs to be a matrix or flowchart added to the guidance section to clarify what devices and associated devices need to be included in a Physical Security Perimeter and what type of monitoring is required for these devices. (b) What is the extent of monitoring of the Physical Security Perimeter that should be implemented; the text seems to indicate the entire perimeter (six wall boundary) needs to be monitored and not just the access points that are required today. This would require complete monitoring of the six sided perimeter with cameras, motion detectors, glass breaks and so forth. This is a substantial change from the current CIP standard and would be a burden on entities to implement and have controls that monitor the PSP 99.9% of the time. We would suggest that if a six wall border can be established than only the access points need to be monitored; otherwise, if a six wall border cannot be established only then, have the entire Physical Security Perimeter monitored. (2) R1.1 – The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "Medium Impact BES Cyber Systems"; otherwise, physical security would be required at all substation with Medium Impact BES Cyber Systems. (3) R1.3 – Replace the words "two or more different physical access control to collectively" to "two factor authentication to" in the requirements. The requirement wordings are confusing and as written may require two different physical access control systems to control access to a Physical Security Perimeters. (4) R1.4 and R1.5 – (a) These requirements require monitoring and alerting for the entire Physical Security Perimeters (PSP) instead of just the access points to the PSP. This requirement needs to be reworded so that if a six-wall border can be established than only the access points to a PSP need to have monitoring and alerting and not the entire PSP. If a six-wall border cannot be established only then require monitoring and alerting for the entire PSP. (b) Add the words "access point" after the words "Physical Security Perimeter" to clarify that you only have to monitor and alarm events on the Physical Security Perimeter access points. (5) R1.4 and R1.6 - These requirements needs to be reworded to remove the 99.9% availability language. Suggest coming up with a more reasonable time frame than 99.9% availability; for example, entity shall have no outage longer than 4 hours for monitoring the Physical Security Perimeters access points. (6) R1.7 – Add the word "detected" in front of the word "unauthorized" in the requirement. This helps clarify the standard on when the 15 minute time frame starts. (7) 3.1 – Add the words "associated with the Physical Access Control system" after the word "devices" in the requirement to clarify what devices need to be tested.
Yes
Yes
Yes
Yes
No
(1) R2.3 – Change 30 days to 35 days in the requirement to match the other requirements in CIP-007. (2) R3.1, R3.2, R3.3, and R4.1 - The words "with External Routable Connectivity or dial-up"

should be added to the applicability after the words "Medium Impact BES Cyber Systems". Currently technology does not exist to meet compliance with these requirements for some serial connected devices; for example programmable protective relays. (3) R3.2 – Add the words "within 35 calendar days" at the end the requirement. There is currently no time frame to mitigate the identification of malicious code and this change would match the other requirements in CIP-007. (4) R4.1 – Add the words "where technically feasible" at the end of the requirement to cover system that cannot log all of the events outlined in R4.1.1-R4.1.4. (5) R4.3 – Reword the requirement to "Activate a response to a human-detected event logging failures before the end of the next business day after the events detection." Changing the requirement gives clarification on when the clock starts for a detected event. (6) R4.4 – Change e the numbers to the bullet format in the Meausres for consistency and match other measures in CIP-007. (7) R4.5 – Performing a sample review every 2 weeks is too tight of a requirement. We would suggest changing the requirement to every 2 months or 3 months to give the entity adequate time to complete the review.
(1) R5.1 – The words "with External Routable Connectivity or dial-up" should be added to the applicability after the words "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) R5.5 – Change the second bullet in the measures to "Documentation that the procedurally enforced passwords meet the password parameters". This would eliminate having to get an attestation from SMEs every time they complete a password change.
Group
Associated Electric Cooperative, Inc (NCR01177, JRO00088)
David Dockery, NERC Reliability Compliance Coordinator, AECI
Yes
Yes
Yes
Yes
Yes
Yes
Yes
[Requirement R7 REPLACE: "by the end of the next calendar day" WITH: "within 24 hours" RATIONALE: Eliminate opportunity for failures due to close but not same timing within same requirement - 24 hours -vs- end of next calendar day. AECI does not feel the benefit is worth industry risk of non-compliance.] [R7 - AECI is also proposing an entire block of changes to the R7.x Rows of the Requirement/Applicability matrix, grouping all of the "For termination actions..." together and ahead of the "For reassignments or transfers...", in order to assist the industry in topically managing CIP requirements based upon employment changes. Please email David Dockery, ddockery@aeci.org, for an electronic copy of those proposed changes.]
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
[Measures R4.1 & R4.5 REPLACE: “signed and dated documentation showing the review occurred”

WITH: “documentation clearly identifying the reviewer and date of review” RATIONALE: Clarification that Entity normative forms of identification, other than electronic or paper signatures, could be acceptable.]
Group
Salt River Project
Sara McCoy
Yes
Yes
Yes
Yes
No
Yes
Yes
CIP-004 R5: This requirement should state that the PRAs need to be updated every 7 years in order to retain cyber access and unescorted physical access. The current wording would indicate that update is required if a PRA was done regardless of whether the person still has access or not.
Yes
Yes
No
Yes
Yes
CIP-006 R1.6: SRP would like clarification regarding this requirement. Does R1.6 require that the Physical Access Control System be within a Physical Security Perimeter? The requirement refers to PACS while the measurement refers to PSP.
Yes
Yes
Yes
No
No
CIP-007 R4 Bullet Point 4.2.2: Is this referring to the identification of any of the events listed in 4.1, or is it referring to the logging mechanism to capture the events? CIP-007 R4.5: SRP requests clarification regarding the 'review' of logged events. Is this a manual review of logged events? SRP believes a manual review every two weeks is a time intensive effort that may not have the intended benefits if too repetitious. SRP suggests a monthly review of logged events.
CIP-007 R5.5: SRP would like to see the verbiage in this requirement changed. SRP suggest using verbiage similar to the CIP-005 R2 which allows for RSA multifactor authentication. This change would allow the option of utilizing multifactor authentication which is actually more secure than only the password complexity now stated in the requirement.
Group
Texas RE NERC Standards Review Subcommittee
Brenda Hampton
Yes
No
No
No
No

No
No
(1) In requirement R2, replace the reference to role-based training with training appropriate to job function. This will eliminate potential confusion about the term “role-based”, which is often associated with IT access control. Suggested wording “Each Responsible Entity shall have a cyber security training program, appropriate to job function, to attain and retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems that includes each of the applicable items in CIP-004-5 Table R2 – Cyber Security Training Program.” (2) For requirements R2.2, R2.3, and R2.4, remove “protecting the Responsible Entity’s BES Cyber Systems”. This reference is already covered more explicitly in the applicability column. (3) Remove requirement R2.10. In complying with requirements R2.1 through R2.9, risks associated with BES cyber security will already be addressed. (4) The following refers to a common concern with CIP-004-5 and recommends various changes to requirements R2 through R7. There are inconsistencies in the applicability requirements of CIP-004-5 regarding requirements for training, PRAs, authorization and revocation for different types of access (physical, electronic, information). The primary concern is that the applicability of Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in all cases due to overriding applicability in other CIP V5 standards. In some instances, the inconsistency can be cleared up by simply changing the applicability from “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” to “Medium Impact BES Cyber System with External Routable Connectivity”. There are several instances where it appears it will be necessary to separate the requirement into two requirements to properly address the applicability concerns. Physical access: Per CIP-006-5 R1, physical access to Medium Impact BES Cyber Systems without External Routable Connectivity should not be subject to the training, PRA, authorization and revocation requirements in CIP-004-5. The inclusion of “dial-up connectivity” in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, R6.3 can be modified to remove the reference to dial-up connectivity in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude dial-up connectivity. This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. A suggested revised definition for Interactive Remote Access is provided in Form D. Information access: The applicability of CIP-011-1 R1 and R2 to Medium Impact BES Cyber Systems is proposed to 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 CIP version 4. Should this proposal be adopted it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 can be modified to remove the reference to dial-up connectivity in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. We would be happy to provide an Applicability Review matrix that includes additional supporting detail if the SDT would like a copy.
(1) In R7.2, replace “…that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer.” with “…one calendar day after the determination that access is no longer needed.” Generally, there is no reason to believe a reassigned or transferred employee is a threat to security and there will be occasion where these employees will need temporary continuing access (e.g. training new employee in position). (2) Refer to comments on question 8 for additional comments on R6 and R7.
Yes
No
In Requirement 1.5, the Measure could be interpreted to prescribe the use of an Intrusion Detection System, however, such a system is not prescribed in a requirement. The references to IDS should be removed. Other systems and tools can be used to detect malicious communications.
(1) The definition of Interactive Remote Access (or applicability of CIP-005-5 R2.1, R2.2 and R2.3) should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal/zero reliability benefit and significant cost associated with applying this

requirement to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of Interactive Remote Access as follows: “All user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol or dial-up. Remote access originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity’s Electronic Security Perimeter(s) or at a defined Electronic Access Point (EAP). Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications.” This definition is also found on Comment Form D, question 12. From V5R1 Consideration of Comments – Definition of EAP section (this helps justify that Interactive Remote Access should not apply to serially connected/non-routable/non-network connected devices): “The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no ‘firewall’ capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs.” (2) In addition, the applicability of CIP-005-5 R2.1, R2.2 and R2.3 should be changed from “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity.”
No
Yes
No
(1) Requirements R1.4 and R1.6 call for 99.9% reliability of monitoring systems. The documentation required to prove this level of reliability and costs associated with this level of reliability would require extensive resources to satisfy. In addition, it’s not clear if these requirements allow for alternate or redundant controls when the primary system is unavailable. For physical access controls, CIP standards should not be so restrictive as to limit options to only electronic methods. The 99.9% availability requirement should be removed and replaced with an allowance for documentation of system maintenance or outages with use of compensatory activities for monitoring. (2) In Requirements 1.5 and 1.7, an exception should be made for system maintenance or outages that last more than 15 minutes so they do not automatically create a violation. During a system maintenance activity such as required patching, the alerting system may not be functional for a period of more than 15 minutes. Unauthorized access may be detected, but not alerted during the maintenance activity. The performance of a required activity such as patching should not put a company in violation of the standard. Allow for documentation of system maintenance or outages and the use of compensatory measures, if required. (3) Requirement 1.7 should be revised from “within 15 minutes of the unauthorized physical access.” to “within 15 minutes of detection.” (4) In Requirement R3.1, remove reference to or provide additional specificity regarding “locally mounted hardware or devices at the Physical Security Perimeter(s)”. This originates within the Physical Access Control System definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. By defining something by what it is not, there is a risk that it may include a number of devices beyond the intended PSP devices. Documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit.
Yes
No
No
No
No
(1) The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. (2) The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected

devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. (3) Under measures, M2.4 bullet 2 should be revised to read “Records of implementation of vendor recommended or other appropriate mitigations;” to eliminate any misunderstanding and allow for appropriate mitigation plans that are different than a vendor-recommended plan. (4) Revise Requirement R3.1 to read “Deploy method(s) to deter, detect, or prevent malicious code within an ESP.”, and Requirement R3.2 to read “Mitigate the threat of identified malicious code within an ESP.” The result is the scope change to include only systems that reside within a “logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.” This would restrict the scope to systems that are capable of utilizing network antimalware products since a routable protocol is being used. An infection to a system where a routable protocol is not being used has minimal impact to BES because the infection has no ability to spread. In addition these systems are not normally susceptible to traditional malware. (5) For Requirement R4.1, modify the requirement to read: “Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events, for applicable BES Cyber Systems which are capable of detecting and logging the events:” to eliminate requirement for those systems where it is not possible to log access events (e.g. legacy relays). (6) Modify Requirement R 4.1.3 from “detected and logged malicious software…” to ”detected and logged malicious code…” (7) Eliminate requirement R4.1.4. The term “malicious activity” is ambiguous. (8) In Requirement R4.2, revise language to replace real-time with an actual target timeframe and refer to capability of the system rather than using the term technically feasible. Suggested language “Issue and alarm or alert, within 15 minutes, for security events that the Responsible Entity determines necessitate an alert, that includes, as a minimum, each of the following types of events where the BES Cyber System is capable:”. Modify Requirement 4.2.1 to read “detected events per R4.1; and”.
(1) Propose change to applicability for Requirement R5.1 to exclude authentication requirements for local electronic access associated with high/med individual serially connected/non-networked/non-routable connected devices. (2) In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read “Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible”. (3) Applicability for R5.2 should be the same as R5.3 – only applicable to external routable connectivity. Change “delegate” to “delegate(s)” as companies may choose to have one or more delegates, depending on how they structure their program. Alternatively, consider removing R5.2 and R5.3 altogether as these requirements may already be covered by CIP-004 R6. (4) In light of the recent RuggedComm vulnerability and backdoor account it appears R5.4 needs to be reworded. The current wording would allow for password similar to the RuggedComm vulnerability. A unique password to a device is find as long as it cannot be determined based upon properties of the device. CIP-007-5 Part 5.4: Recommended change, “Change known default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” This allows for unique passwords. (5) CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold.
Individual
Daniel Duff
Liberty Electric Power LLC
Yes
No
No
No
No
Yes
Yes
The standard still does not have a mechanism which allows for a vendor controlled cyber security system. Suggested language: A Registered Entity allowing cyber access to a vendor providing support services shall be deemed in compliance with Requirements 2 through 5 of this standard if all of the following criteria are met 1) the vendor has instituted a cyber security program which contains all of

the elements detailed in Requirements 2 through 5 of this standard; 2) the vendor has provided the RE a list of employees authorized for cyber access prior to gaining access to the asset; 3) there is a methodology for confirming the identity of the vendor employee at the time of access and 4) access to the asset remains in control of the RE at all times (through control of such means as a physical connection to the asset). This would allow REs to continue to receive vendor support for trip analysis, troubleshooting, etc and avoid long travel time delays before returning a unit to service. This requirement is another example of the huge problem of "mission creep" within the standards. When initially written, the standard was not designed to apply to small entities which rely on outside vendors for support services. The Risk Based Assessment was used to filter out those REs. Today, we see the same standard language, but the Risk Based Assessment has been replaced with criteria which will potentially capture many small merchant companies which pose little risk to the BES. (Example - a company with 310 Mw of peaking plants with one control room and two locations). The SDT must recognize that not every power producer controls thousands of Mw of generation, and that provisions for independent producers that reflect the realities of the business must be written into any standard that covers these entities.
Yes
No
Multi-factor recognition gains little in reliability and should not be a requirement.
No
Yes
Yes
The requirement for "99.9% availability" needs further definition. As written, the time period "24 hours a day/7 days a week" is the only time frame noted in the standard. 99.9% availability for any particular week would mean a ten minute outage of a system would put an entity into violation space.
Yes
Yes
Yes
Yes
No
Disagree with the proscription for passwords. Password formatting has a history of rapid change, and codifying a system into a standard which can take years to change is an unforced error. Further, less complex passwords can have greater degrees of entropy than the system proposed, so an entity could impose requirements which are much stronger than the standard requires, but be in violation of the standard.
Group
Colorado Springs Utilities
Jenn Eckels
Yes
Yes
Yes
No
Yes
Yes
No
Table R4: Personnel Risk Assessment Program: Colorado Springs Utilities would like more clarification on what level is required of the documented criteria (specific convictions, time passed since conviction, severity, etc.). Also, we are concerned that the documented criteria must also adhere to other laws and regulations. For example, creating a screening matrix weeding out those with criminal offenses based on legally defensible reasons (nature and gravity of the offense, time passed since

conviction and/or completion of sentence, nature of the job held or sought) has a high risk of adversely impacting those in a protected class.
Table R7.1: Access Revocation: Colorado Springs Utilities believes that the language in the requirement table seems to contradict the Change Rationale table.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Group
Family Of Companies (FOC) including OPC, GTC & GSOC
Guy Andrews
Yes
Yes
No
Yes
Yes
Yes
No
(R1)The drafting team should make clear in the Guidelines and technical basis section what the term "Responsible Entity's personnel" is intended to mean. Is this only employees of the Responsible Entity or does it also include contractors and vendors? (R2) The drafting team should consider combining CIP-004-5 R2 parts 2.7 and 2.9. Initial notifications, discussed in 2.7, could be considered part of the response action identified in 2.9. At the very least, these two parts should be listed consecutively to improve readability. (R3) R3 should make clear who needs to receive the training. The requirement itself mentions only access to BES Cyber Systems, but the applicability of the parts identifies other systems. However, the language in the part itself is ambiguous. Recommend modifying the language in the main requirement of R3 to state "applicable BES Cyber Systems and associated Cyber Assets" to match the heading of the table. (R4) See comment regarding R3 about ambiguous language.
(R6) Recommend a corresponding annual review that provisioned physical security privileges are those that a Responsible Entity determines necessary for performing assigned work functions. (R7) We disagree with the requirement to initiate the process to revoke access "upon the effective date and time" of the termination action. This language obligates the Responsible Entity to initiate this action precisely on this date and time. Initiating this process prior to would not meet the definition of "upon." Additionally, this obligates the entity to demonstrate that it met 2 distinct timetables "initiated…upon" and "complete…within 24 hours." We understand the intent is to encourage the entity to begin the process immediately, consistent with FERC Order 706, but we believe the drafting team has inadvertently set up a compliance trap for the industry. We recommend this language be changed to "For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access as part of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. (R7 - part 7.5) We question the need to modify passwords for shared user accounts if there is no corresponding

requirement to disable individual accounts for the user who was reassigned or transferred. Additionally, as passwords are not a required authentication mechanism, we recommend that this requirement be modified to "change any shared authentication factors that are known."
No
No
(Part 1.1) The text of the requirement part includes "associated Protected Cyber Assets" but the applicability does not. Please clarify. (Part 1.5) Part 1.5 states that each entity must have a method for detecting malicious communications. This is vague. What level of detection is required? Would simply having log entries sent to a server for analysis be sufficient? Would it be sufficient if combined with a MSP service? The measures imply that only IDS would suffice, but entities have a right to more than an implication of what is required. If the SDT wants to require IDS, then it should be clearly stated. If not, it should provide a measurable standard of what level of detection is required. IDS devices could be incorporated into an access point, or located within an ESP; therefore the applicability only to EAPs may not be appropriate.
It is not clear whether the entire chain,: from user to Intermediate Device, and from Intermediate Device to Cyber System, must be encrypted or only one of the links. Please clarify.
No
Yes
Yes
(R1) We strongly disagree with requirement parts 1.4 and 1.6. Given the large number of field assets that are applicable to this requirement, a 2 hour monitoring outage that occurred more than 4 times in a year for any single facility would mean violation with this requirement. A single chronic communications circuit would easily put many entities into a non-compliant state. We recommend that CIP-006 utilize the same strategy employed in CIP-007 R4, part 4.3 - requiring the detection of failures and activating a response. We believe this incentivizes the proper behavior without causing unnecessary compliance issues. (Part 1.1 and Part 1.3) The requirement for two physical access controls goes beyond current industry standards and is not sufficiently connected to increased reliability to justify the expense involved. The definition of physical access control is not sufficiently clear. The language Physical Security Perimeter has been restored to the requirement, but there is no requirement to actually establish a PSP or a statement as to what devices must be within a PSP. We recommend that R1.1 be modified by adding “into each Physical Security Perimeter”. (Part 1.4) R1.4 Controls should control things; not monitor things. We recommend deleting the words “Have controls that” or changing them to “Implement measures to”. Automated systems typically cannot detect unauthorized physical access because they cannot distinguish between authorized key access and unauthorized key access. Consider adding the word “potential” before “unauthorized” if your intent is to monitor for events that may be unauthorized circumvention of a physical access control, such as a “forced open alarm” which could be the result of an authorized key entry or true forced entry. (Part 1.5) R1.5 Note that R1.5 does not require alerting on repeated invalid access attempts. Since access was denied, the control has not been circumvented. We do not object to this approach, but we want to be certain that this was the intent of the SDT. (Part 1.6) It is not clear what an entity is supposed to do to meet this requirement. How does one detect unauthorized physical access to a Physical Access Control System? Especially since the standard rationale for R1.1 states that Physical Access Control Systems do not themselves need to be protected by a Physical Access Control System. In light of this statement the measure for 1.6 makes no sense.
No
Yes
No
Yes
Yes
(Part 1.1) R1.1 requires that only needed ports be enabled. This implies that an entity must be able to justify the assertion that a port is needed. But the measures make no mention of the inclusion of the application for each port. It should be made clear, one way or another whether you are looking for a simply listing of the ports, or whether an entity needs to document the purpose or application of each port. (Part 1.2) The requirement is vague. It does not make clear what level of protection is required. The measure attempts to add more detail, but that is not the correct purpose of a measure;

if disabling the port in software, using a physical port lock or signage are the three possible solutions they should be included as such in the requirement. If those are not the only three possibilities entities need more specific information about what level of protection is required. Allowing protection via signage makes the requirement of little value. What is the reliabiliy benefit of having signage for physical ports? The standard requires protection only of unnecessary physical ports. The term unnecessary is vague. Many, if not most, physical console ports are used only for initial programming and then remain available for emergencies. If these ports are covered then the requirement is contrary to reliability because it encourages disabling or physically locking these ports that are already located in secure areas and can be critical for restoring failed systems. This requirement will delay or prevent responses to system failures in that case. If these ports are not covered then what is the point of the requirement? (Part 3.1) R3.1 is vague. It does not make clear what is required to meet it. Would a corporate policy stating that employees should not visit sites known to be sources of malware be sufficient by itself? The measures make some attempt to add detail (which is not the purpose of a measure), but even they are vague. For example, what constitutes “system hardening”, and “policies” could be almost any appropriate use policy. (Part 3.2) R3.2 is vague as well. What level of mitigation is required? We already mitigate this threat by the measures required by CIP 5 (limiting active ports on the perimeter). If that is enough, this requirement is duplicative; if it is not, how is an entity to know what additional steps are required? (Part 4.1) R4.1.4 is vague. What activities, beyond those listed in 4.1.1-4.1.3 would be included? (applies to 4.2.1 as well)
(Part 5.1) For systems not associated with control centers, please clarify that "user access" does not include the ability to interact with the LED/LCD panel on the front of a device (such as a protective relay or meter).
Individual
Brian J Murphy
NextEra Energy, Inc.
No
No
No
No
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 R1.1 be revised to read as follows: “A security awareness program that, at a timeframe deemed necessary by the Responsible Entity, conveys ongoing reinforcement of cyber security practices for the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. “ And, also R3.2 to be revised to read as follows: “Require completion and documentation of the training specified in CIP-004-5, Requirement R2 as deemed necessary by the Responsible Entity.” Also, R4.2 should be revised to require that the Responsible Entity have a current criminal background check, and not impose or suggest arbitrary timeframes that unnecessarily and overly complicate or micromanage the intent of the requirement. R4.2 should be revised to read as follows: “A current and up-to-date criminal history as the Responsibility Entity deems necessary.” Similarly, R5.2 should read as follows: “A current and up-to-date PRA with no lapses in criminal history, unless such lapses are justified and documented.”
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 micromanagement of the program. To implement these changes, NextEra requests that R6.5 be revised to read as follows: “Verify, at a timeframe that the Responsible Entity deems necessary, that individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records. “ Similarly, revise R6.6 and R6.7 to read as follows: “For electronic access, verify, at a timeframe that the Responsible Entity deems necessary,

that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions." "Verify, at a timeframe that the Responsible Entity deems necessary, that access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity are correct and those that the Responsible Entity determines necessary for performing assigned work functions. " Also, to provide for the recognition of extenuating circumstances (such as a hurricane or some other unforeseeable event), R7.1 and R7.3 should be revised to read as follows: "For all termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action, unless there are extenuating circumstances that impact the completion of the revocation within 24 hours and such extenuating circumstances are documented." "For termination actions, revoke the individual's access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity by the end of the next calendar day following the effective date and time of the termination action, unless there are extenuating circumstances that impact the completion of the revocation within 24 hours and such extenuating circumstances are documented." Also, it is unclear what the wording of R7.2 means. While it may be understood the language is mirroring FERC's directive, it is generally understood that a Responsibility Entity needs flexibility to prioritize and implement compliance in a manner appropriate for the circumstances and situations. For example, for any employee that is reassigned for disciplinary reasons, a tight timeframe is appropriate, but for a normal employee transfer such a tight timeframe is unnecessary and inappropriately places an emphasis on revocation versus other aspects of the CIP program. Thus, additional flexibility, as appropriate, needs to be added to R7.2 as follows: "For reassignments or transfers involving disciplinary action, revoke the individual's electronic and physical access that by the end of the next calendar day following the reassignment or transfer, and for reassignments or transfers that do not involve disciplinary action, revoke in timeframes as deemed appropriate and documented in a procedure by the Responsible Entity."
No
No
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference.
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 R3.2 be revised to read as follows: "Document outages for physical access control, logging, and alerting systems and retain the outage records for a time period as deemed necessary by the Responsible Entity." Also, NextEra does not take issue with the applicability sections of CIP-006-4 R1.3 through R1.6 or R3.1 or conceptually what the requirements are attempting to accomplish, but Nextera does believe that these requirements need to be revised in order to practically and cost effectively promote reliability and physical security. Thus, NextEra provides specific edits and a justification for the edits below for each of these requirements. R1.3 (edited) "Utilize one physical access control and one defense in depth control to allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access." NextEra believes that requiring two physical access controls or a technical feasible exception is unnecessarily redundant and does not promote cyber security in a practical or cost effective manner. Instead, NextEra is confident that requiring one physical access control and one defense in depth control is appropriate and will protect against unauthorized physical access. It is also NextEra's view that these two controls should be required, and, therefore, the technical feasibity exception language has been deleted. R1.4 (edited) "Have a control, as required in R1.3, that monitors the Physical Security Perimeter twenty four hours a day, seven days a week for unauthorized circumvention of a physical access control into a Physical Security Perimeter. In the event of an outage of the control, the Responsible Entity must take appropriate action to ensure there is no unauthorized circumvention into

the Physical Security Perimeter during the duration of the outage. The Responsible Entity must document the temporary approach used during the outage of the control, and document that no unauthorized circumvention into the Physical Security Perimeter occurred during the outage." NextEra agrees that 100% perfection is not possible, given the possibility of a malfunction or damage to a Physical Security Perimeter control. NextEra does not agree with the use of an unsupported, arbitrary 99.9% threshold. Instead, NextEra believes the same goal of security is accomplished if an appropriate reaction to the temporary outage of a control is taken and documented. Thus, NextEra recommends that its edits to R1.4 and R1.6, below, be employed instead of the 99.9% threshold. R1.5 (edited) "Within 15 minutes of an employee or agent of the Responsible Entity becoming aware that a Physical Security Perimeter has been breached by an unauthorized circumvention of a physical access control, the Responsible Entity shall issue an alarm or alert on the unauthorized circumvention of a physical access control to the personnel identified in the BES Cyber Security Incident Response Plan." Although NextEra agrees with the intent of R1.5, as worded it is not clear what is required by whom and when the 15 minutes starts to run. Thus, NextEra recommends that its edits to R1.5 be adopted to better explain the step-by-step process of the event and the action to be taken. R1.6 (edited) "Have a control, as required in R1.3, that monitors the Physical Security Perimeter twenty four hours a day, seven days a week for unauthorized circumvention of a physical access control into a Physical Security Perimeter. In the event of an outage of the control, the Responsible Entity must take appropriate action to ensure there is no unauthorized circumvention into the Physical Security Perimeter during the duration of the outage. The Responsible Entity must document the temporary approach used during the outage of the control, and document that no unauthorized circumvention into the Physical Security Perimeter occurred during the outage." R3.1 (edited) "Maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter shall be conducted at least once every 36 calendar months to ensure the control, hardware or device properly function." NextEra finds no justification for increasing the maintenance and testing of each Physical Access Control System and locally mounted hardware or devices at the Physical Security Perimeter from 36 months (as is currently required in CIP-006-3) to 24 months. Although NextEra does not question the importance of maintenance and testing required in R3.1, its experience demonstrates that during a three year test of each Physical Access Control System and locally mounted hardware or devices, only minor, if any, issues are detected. These results suggest that any increase in testing intervals is not required to promote reliability or cyber security. Also, such an increase in testing intervals unnecessarily negatively impacts the cost effectiveness of implementing a cyber security compliance plan. In addition, NextEra believes that the R3.1 grammar and clarity can be improved. Accordingly, NextEra recommends that its edits to R3.1 be adopted.
No
No
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 R.4.4 and R4.5 be revised to read as follows: "Retain BES Cyber System security-related event logs identified in Part 4.1 for a time period as the Responsible Entity deems necessary and where technically feasible." "Review a summarization or sampling of logged events at a timeframe as deemed necessary by the Responsible Entity to identify undetected Cyber Security Incidents."
NextEra supports EEI's comments on this requirement, and incorporates them herein by reference. As a preferred alternative to EEI's comments, 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 R.5.6 be revised to read as follows: "For password-based user authentication, either technically or procedurally, that enforces password changes or an obligation to change the password at a timeframe deemed necessary by the Responsible Entity."
Individual

Michael Lombardi
Northeast Utilities
Yes
No
No
Yes
Yes
Yes
No
R2 and R3 – Recommend that Requirement R2 and R3 be revised to specify a general awareness training program is necessary to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. As currently proposed, requiring a role-based cyber security training program to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems is problematic and provides little or no corresponding benefit. For example, a potentially problematic condition includes how to handle granting access to employees that have more than one role yet have only completed training for one role only – would they qualify for unescorted physical access or not? Similarly, as personnel are assigned new / additional roles, is their unescorted access jeopardized based on their increased responsibility? FERC Order 706, Para 434 does not specify role based training but indicates: “We [FERC] agree with commenters that information concerning vulnerabilities should be revealed on a need to know basis and not universally. However, any employee with access to an area where his or her actions, or carelessness, could put critical assets at risk, should receive the necessary training to assure that the employee understands how his or her actions or inactions could, even inadvertently, affect cyber security.”
R7 – While Part 7.5 addresses that the Responsible Entity can determine and document that extenuating operating circumstances require a longer time period for changing passwords; it does not appear that a similar provision exists to allow the Responsible Entity to determine and document that extenuating operating circumstances can require a longer time period for revocation of access privileges. Recommend that Requirement R7 be revised (pursuant with FERC Order706, Para 463) to acknowledge that the Responsible Entity can determine and document that extenuating operating circumstances require a longer time period (beyond the default 24 hours) for the revocation of access privileges. FERC Order 706, Para 463 states: “We [FERC] acknowledge that not all disciplinary actions warrant revocation of access privileges. In addition, certain personnel transfers can require a protracted transitional process that warrants retention of access privileges after the formal transfer date. There may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes.”
Yes
Yes
None
Request clarification on R2 Part 2.2 - Is the entire link from field device to desktop user required to be encrypted, or just the desktop to intermediate device, or field device to intermediate device?
No
Yes
Yes
Table R1, Part 1.6 - Requires 99.9% availability yet no availability methodology or time frame is provided. Please clarify how the availability calculation should be performed. A simple example of the need for clarification is: a physical access control system is unavailable for 4 hours on one day but is available for the remainder of the year. Hence daily availability = 83.33% (20/24 hours), weekly availability = 97.62% (164/168 hours), and the annual availability = 99.95% (8756/8760). Additionally, please clarify the applicability of this requirement, e.g., is it to the overall control system or each individual door, panel, etc? Please clarify how scheduled outage time is handled (and whether it is excluded from the availability calculation). Lastly, please provide the basis for 99.9%.
Yes
Yes

Yes
Yes
Yes
Table R1, Part 1.2 - Suggest Measure be revised to remove “signage” as an alternative to physically securing a port. Table R2, Part 2.4 - Appears change rationale is from Part 2.2 and does not address 2.4. Table R3, Part 3.3 - suggest rewording from “(this does not require use of every available release, but that for every release that is available, at least one update has occurred within 35 calendar days from that release)” to “(this does not require use of every available release, but that for every release that is applicable, at least one update has occurred within 35 calendar days from that release). Table R4, Part 4.2 - Suggest “real-time” be removed as determinations are not made in real time. Rather, events are capture and evaluated. Table R4, Part 4.5 - Consideration of Comments from the prior posting indicated “Responsible Entities may engage in automated or manual review in accordance with their current or future capabilities.” The flexibility and the allowed use of automated reviews is appreciated. Application Guidelines - Please provide more details in the Application Guidelines on TFEs that may be allowed on equipment that does not run malicious code Request clarification on R4, Parts 4.1.1, 4.1.2, 4.1.3, 4.1.4 - Are log events required for local, remote or both types of access?
None
Group
Florida Municipal Power Agency
Frank Gaffney
Yes
Yes
Yes
Yes
Yes
No
No
(1) Question 5: The end of the sentence of bullet 5.2 should be changed to include “calendar”, e.g., “no older than seven calendar years”.
(1) Question 6: R6 has too many proscriptive internal controls within the bullets that should be eliminated, especially in light of paragraph 81 of the FERC Order approving Find Fix Track and Report, e.g., there is no need to designate individuals able to authorize, etc. Bullets 6.6 and 6.7 are unnecessary and are redundant to 6.5. In other words, 6.6 and 6.7 are too proscriptive for how to accomplish 6.5. (2) Question 7: Bullet 7.1 is impossible from a temporal perspective. It is impossible to “initiate the process to revoke … upon the effective … time of the termination action”, literally meaning simultaneity which is impossible to achieve. The only important part to the bullet is to revoke access within 24 hours and the rest should be eliminated.
Yes
Yes
No
No
No
(1) Question 14: See comments on definition of Physical Security Perimeter. Bullets 1.7 and 1.8 could be interpreted as requiring continuous availability of alarming and logging systems. FMPA suggests adding the 99.9% availability used in bullet 1.6 to bullets 1.7 and 1.8 as well. Bullet 1.9 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. READ-ONLY ACCESS There is no provision for a “read only” version of electronic access without meeting the requirements for unescorted electronic access. We believe that there ought to be a method for “escorted” electronic access, e.g., read-only access, e.g., something akin to WebEx – if you let someone view your screen

but don't give them control, that would be a form of "read only" supervised access. This kind of access should be encouraged, for a number of reasons, including: 1) Having this form of 'read only' access makes it easier for companies to get support on issues without having to worry about a litany of training & background check issues 2) By not having so many people with access to critical assets, it obviously lowers the number of people on your lists which makes tracking people less of a burden. Also by keeping the list smaller you inherently gain security. 3) Assuming you have internal employees actually performing the access (or "driving", if you will), it has the potential for them to increase their comprehension of how things work, thereby creating a more robust BES by having better educated operators 2- QUESTION 15: Bullet 2.1 is not measurable without video surveillance or similar surveillance. Continuous is impossible to prove without such surveillance. Is that the intent of the SDT? The Measure does not match the Requirement. 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. 3- QUESTION 16: The second part of Bullet 3.2: "and retain the outage records for at least 12 calendar months" 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.
No
Yes
Yes
No
No
1- QUESTION 18: For CIP-007-5 bullet 1.1, the auditors have taken the word "services" to mean "applications" running on a computer. Which means right now they expect you to show all the things that MIGHT start on a Windows (or Unix) box, and if they're not needed, disable them. We believe the SDTs intent is concerning network communications and not services like those that automatically configure to connected hardware. We suggest to include the following language in the bullet: "that initiate or receive network communications" after "services", i.e: "For applicable Cyber Assets and where technically feasible, enable only logical network accessible ports needed, including port ranges or services that initiate or receive network communications where needed to handle dynamic ports." 2- QUESTION 21: Bullet 4.1 implies a 100% availability of a logging system. FMPA suggests using the 99.9% availability used in CIP-006-5 Bullet 1.6. Bullet 4.4 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.
QUESTION 22: Bullet 5.2 is an internal control not worthy of a requirement, especially in light of paragraph 81 of the FERC Order approving Find Fix Track Report. FMPA suggests deleting the bullet.
Individual
Yuling Holden
PSEG
Yes
Yes
Yes
Yes
No
Yes
Yes
In R5.2, change the measure "Evidence may include, but is not limited to, current and previous personnel risk assessment records" to delete the word "current." There is no benefit to keeping records that may go back 14 years.
Yes
No
We are struggling with dial-up applicability as it relates to interactive remote access. Specifically, is a

dial-back modem can be considered as an Intermediary Device? If it is, then there are difficulties in meeting complying with R2 (such as 2.3 and 2.2). If it is not, then how can it be an option within R1 (R1.4)?
No
Yes
Yes
R1.6: Monitoring 24*7*365 with a 99.9% uptime would require extensive resources to satisfy the supporting documentation. Please provide a basis for the requiring a 99.9% uptime. Also, we are looking to clarify the method that is used to calculate the percentage of availability for our systems. For example: If a badge reader is malfunctioning, but the door is locked, so no access is granted, would this count as an outage, as the security of the site was not compromised? With regard to the Measure for R1.6: It seems that there is a significant difference between the Requirement and the Measure. We propose the following language in the Measure to appropriately correlate the two: instead of “Evidence may include, but is not limited to, documentation of controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.” We propose “Evidence may include, but is not limited to, documentation of controls that monitor the Physical Access Control System.”
Yes
Yes
Yes
No
Yes
For Requirement R4.5, Please provide guidance as to what acceptable tolerance range for such sampling. Once this clarification is provided, our objection would be removed VSLs: R1: There is only a Severe VSL. We would like to see a gradation with regard to the VSLs – If a single device is affected, there may be less severity than if many devices are affected. R2 -R3: R2 escalates by 15-day increments and R3 escalate by 10-day increments. We believe there should be consistency across similar VSLs. General comment on requirements with only a Severe VSLs: There should be gradations that include lower VSLs on the basis of the difference between missing a subset of the devices or systems and missing all of such systems.
Group
Pepco Holdings Inc & Affiliates
David Thorne
Yes
Yes
Yes
Yes
Yes
No
Yes
1) Q6—R6 -NOT CLEAR: individuals provisioned for authorized electronic access or authorized unescorted physical access have associated authorization records. Change Rational: This requirement clarifies the review should occur between the provisioned access and authorized access. What review? Are they not 2 different authorizations?
Yes
Yes
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Yes
Group
National Rural Electric Cooperative Association (NRECA)
Barry Lawson
No
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Individual
Jennifer Wright
San Diego Gas & Electric
No
No
Individual
Don Jones
Texas Reliability Entity
Yes
Yes
Yes
Yes
Yes
Yes
No
CIP-004-005 Table R7 part 7.4 should be deleted. Allowing 30 calendar days is excessive. CIP-004-005 Table R7 part 7.5 should include Medium Impact BES Cyber Systems.
Yes

Yes
No
Yes
No
R1.7 does not indicate follow up on the unauthorized access alert by the personnel identified in the BES Cyber Security Incident Response Plan. R3.1 should be tested annually.
Yes
Yes
Yes
Yes
Yes
Individual
Don Schmit
Nebraska Public Power District
Yes
No
No
Yes
Yes
Yes
No
[R1] though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] Each type of role-based training, 2.2-2.10, should be optional for some identified roles and required for others, and that distinction should be programmatically documented. That needs to be clearer in the structure of this requirement. If each of 2.2 through 2.10 were preceded with “Based on the role identified in R2.1…“ The way this is written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. More specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [R4] With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit.
R7.2: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need

to straddle two jobs until a replacement is up to speed. R7.3: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. R7.4: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. : If disabling their domain accounts and physical access effectively terminates access, do we still need the urgency of 24 hrs? I understand the logic behind this but would rather see this as a 30 day requirement. R7.5: The "out" for extenuating operating circumstances should be applied to all CIP 4 R7 requirements.
No
Yes
[R1.1] Proposed verbiage change for the applicability. R1.1 “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. The requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken.
None.
No
Yes
Yes
R1.2 Ensure applicability statements clarify that the associated EAC and Protected Cyber Assets are those associated with Medium Sites. R1.4 –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are audit bait that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. R1.5: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. R1.6 The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. R1.7: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans.
Yes
No
No
No
No
Ensure the “zero defect” language in the VSLs is changed to be in alignment with EEI comments and the requirements, themselves. [R1.1] Propose defining “network accessible” to clarify the requirements around the additional controls offered by firewalls and ports accessible only to the local host and whether those controls can be considered sufficient. Also recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. [R2.4] Recommend adding flexibility to change the plan without risking

non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the planned and actual implementation.” [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Ensure “High” is a qualifier for each of the systems identified in the applicability column. Proposed Verbiage to add clarity: “Document and implement a program to review a summarization or sampling of logged events, at a minimum, every two weeks, to identify un-alerted Cyber Security Incidents.” Rationale – with the documentation of a program, the entity can define the criteria for sampling and summaries without risking a finding of non-compliance when not meeting the interpretation-based expectation of an auditor.

[R5.1] Propose change to “within the capability of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change default passwords, unless the default password is unique to the device or instance of the application.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…”

Individual

AnthonyJablonski

ReliabilityFIrst

CIP-004-5 1. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the ”Severe” VSL to state: “failed to implement its documented” to be consistent with the language in Requirement R1. This recommendation is based on the 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. 2. VSL for Requirement R2 a. A reference to Part 2.1 (Identification of each role and training required for each role) is missing from the VSLs. If a responsible entity failed to include Part 2.1 in their training program, it is unclear what VSL category the responsible entity would fall under. ReliabilityFirst recommends adding a VSL which is associated with Part 2.1. b. The “High” VSL should be revised to reference missing “3 or more.” As stated in the current VSLs, the “Moderate” VSL jumps from missing “2 or more” to missing “4 or more” in the “High” VSL. 3. VSL for Requirement R3 a. The SDT may want to consider making the VSLs size natural similar to the way the VSLs for CIP-002-5 Requirement R1 are set up. For example, for Responsible Entities with more than 40 individuals use percentages and for Responsible entities with less than 40 individuals use a finite number. In some instances, applying a fixed number to an entity with a large size may result in a determination of violation that is higher or lower than might have been intended. Similarly, applying a percentage to an entity with a small size may result in grading a violation higher or lower than might be intended. 4. VSL for Requirement R4 a. There appears to be a typo in the “High” VSL. The reference to the parenthetical (4.5) should correctly point to (4.4). There is no Part 4.5 listed in the Requirement R4 table. 5. VSL for Requirement R5 a. ReliabilityFirst recommends modifying the “Severe” VSL to state: “The Responsible Entity failed to implement one or more documented processes for personnel risk assessments. (R5)” to be consistent with the language in Requirement R5. b. The SDT may want to

consider making the VSLs size natural similar to the way the VSLs for CIP-002-5 Requirement R1 are set up. For example, for Responsible entities with more than 40 individuals use percentages and for Responsible entities with less than 40 individuals use a finite number. In some instances, applying a fixed number to an entity with a large size may result in a determination of violation that is higher or lower than might have been intended. Similarly, applying a percentage to an entity with a small size may result in grading a violation higher or lower than might be intended.
CIP-004-5 VSLs 1. VSL for Requirement R6 a. ReliabilityFirst recommends modifying the “Severe” VSL to state “…failed to implement one or more documented...” to be consistent with the language in Requirement R6 2. VSL for Requirement R7 a. ReliabilityFirst recommends modifying the “Severe” VSL to state “…failed to implement one or more documented...” to be consistent with the language in Requirement R7. This recommendation is based on the 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. b. For the “Moderate”, “High” and “Severe” VSLs, why is the following standard number and requirement number specifically spelled out in the VSL: “CIP-004-5 R7”? To be consistent with the format other VSLs, ReliabilityFirst recommends removing this language.
CIP-005-5 1. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the first “Lower VSL” to state "failed implement one or more documented processes" to be consistent with the language in Requirement R1. Furthermore, ReliabilityFirst recommends moving this “Lower” VSL to the “Severe” category. If a Responsible Entity failed to implement one or more documented processes that collectively include each of the applicable items in CIP-005-5 Table R1, ReliabilityFirst believes that entity has completely missed the intent of the requirement and should be “Severe” b. The VSL under the “Severe” category which states “External Routable Connectivity through the ESP was not through an identified EAP according to Requirement R1, part 1.2.” appears to be incomplete. ReliabilityFirst recommends modifying the VSL by adding the following language to the beginning of the VSL to make it a complete thought: “The Responsible Entity did not have all…”
CIP-005-2 VSL 1. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Lower” to state: "failed to implement one or more documented processes" to be consistent with the language in Requirement R2. Furthermore, ReliabilityFirst recommends moving this VSL to the “Severe” category. If a Responsible failed to implement one or more documented processes that collectively include the applicable items, where technically feasible, in CIP-005-5 Table R2, ReliabilityFirst believes that entity has completely missed the intent of the requirement and should be “Severe”. b. ReliabilityFirst recommends adding the last bullet under the “Severe” category as a bullet under the “High” category as well (i.e. if you missed one of the three bullets you are a “High”. If you miss two of the three bullets you are a “Severe”).
CIP-006-5 1. VSL for Requirement R1 a. The second “High” VSL (the one dealing with Part 1.6) needs to have the erroneous word “has” removed from the beginning. ReliabilityFirst recommends the following: “The Responsible Entity does not have controls that monitor…” b. The fourth “Severe” VSL (the one dealing with Part 1.4) needs to have the erroneous word “has” removed from the beginning. ReliabilityFirst recommends the following: “The Responsible Entity does not have controls that monitor…” 2. VSLs for Requirement R3 a. To add further clarity to the “Moderate” VSL, ReliabilityFirst recommends the following: “The Responsible Entity has documented and implemented a maintenance and testing program for Physical Access Control Systems, but the testing was not performed on a cycle within 24 calendar months. (3.1)”
CIP-007-5 1. General comments on all VSLs 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. 2. VSL for Requirement R1 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R1. This recommendation is based on the 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. 3. VSL for Requirement R2 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R2. This recommendation is based on the 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. 4. VSL for Requirement R3 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R3. This recommendation is based on the 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. 5. VSL for Requirement R4 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R4. This recommendation is based on the 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.
CIP-007-5 1. VSLs for Requirement R5 a. ReliabilityFirst recommends modifying the first “Severe” VSL to state: “…failed to implement one or more documented...” to be consistent with the language in Requirement R5. This recommendation is based on the 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. b. It appears a number of the Parts listed in the CIP-007-5 Table are not mentioned in the associated VSLs. The language in the VSLs needs to be consistent with the language in the associated Parts and cannot add requirements. For example it is unclear which VSL corresponds to Part 5.2. There is no mention of a “CIP Senior Manager or delegate” in any of the VSLs.
Individual
Christina Conway
Oncor Electric Delivery Company LLC
Yes
No
No
No
No
No
No
APPLICABILITY COMMENTS THAT APPLY TO CIP-004-5 R2 THROUGH R7: (1) There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. (2) Oncor’s primary concern is that the applicability of “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. As Oncor describes below, in some instances the inconsistency can be cleared up by changing the applicability from “Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity” to “Medium Impact BES Cyber System with External Routable Connectivity.” (3) There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. (4) Physical access: Per CIP-006-5 R1, physical access to “Medium Impact BES Cyber Systems without External Routable Connectivity” should not be subject to the training, PRA, and authorization and revocation requirements in CIP-004-5. The inclusion of “dial-up connectivity” in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, and R6.3 should be modified to remove the references to “dial-up connectivity” in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, and R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. (5) Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude “dial-up connectivity.” This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. (6) Information access: There are inconsistencies between CIP-004-5 and CIP-011-1 with respect to the applicability of BES Cyber System Information requirements. CIP-004-5 R2.3, R6.1, R6.4, R6.7 and R7.3 should be modified to match the applicability of CIP-011-1. Additionally, if a change that Oncor in proposing to CIP-011-1 R1 and R2 is accepted, then there will be further inconsistency between CIP-004-5 and CIP-011-1 that should be reconciled. In its comments to CIP-011-1, Oncor proposes that the applicability 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 CIP version 4. If Oncor's proposal for CIP-011-1 is adopted, it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue, the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 should be modified to remove the reference to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. R2 REQUIREMENT COMMENTS: The phrase "protecting the Responsible Entity's BES Cyber Systems" should be removed from the end of CIP-004-5 R2.2, R2.3 and R2.4 since applicability is addressed in the applicability column of each sub requirement. This change will also make R2.2, R2.3 and R2.4 consistent with the other R2 sub requirements. FURTHER R2 APPLICABILITY COMMENTS: There is an inconsistency between the applicability of CIP-004-5 R2.8 and CIP-009-5 that should be corrected so that the applicability of both sections match. Both CIP-004-5 R2.8 and CIP-009-5 address recovery plans; thus their applicability logically should be the same. In its comments on CIP-009-5, 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 change would concentrate the efforts of Responsible Entities on areas where the potential reliability impacts are the highest and would avoid the implementation of Standards that place additional/duplicate requirements on cyber systems/assets covered under the PRC standards. If Oncor's proposal for CIP-009 is adopted, it will become necessary to adjust the applicability of CIP-004-5 R2.8 by replacing "Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity" with "Medium Impact BES Cyber Systems at Control Centers." R3 REQUIREMENT COMMENTS: The reference to "BES Cyber Systems" in CIP-004-5 R3.1 should be changed to "applicable cyber assets" to maintain consistent use of the applicability column. 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.

APPLICABILITY COMMENTS THAT APPLY TO CIP-004-5 R2 THROUGH R7: (1) There is general inconsistency among the applicability of requirements in CIP-004-5 with respect to how they apply to training, personnel risk assessment, and authorization and revocation requirements for different types of access. The applicability of each requirement should be reviewed from a functional perspective to determine how it applies to different types of physical, electronic, and information access. (2) Oncor's primary concern is that the applicability of "Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity" is applied to all CIP-004 R2 through R7 requirements. This is not appropriate in many requirements due to the overriding applicability of other CIP V5 Standards. As Oncor describes below, in some instances the inconsistency can be cleared up by changing the applicability from "Medium Impact BES Cyber System with External Routable Connectivity or Dial-up Connectivity" to "Medium Impact BES Cyber System with External Routable Connectivity." (3) There are also several instances in which different types of access are addressed within the same requirement. Due to the varying applicability of different access types, it appears it will be necessary to separate these requirements into multiple requirements to properly address the applicability concerns. (4) Physical access: Per CIP-006-5 R1, physical access to "Medium Impact BES Cyber Systems without External Routable Connectivity" should not be subject to the training, PRA, and authorization and revocation requirements in CIP-004-5. The inclusion of "dial-up connectivity" in the applicability column of requirements related to physical access goes beyond the intended applicability in CIP-006-5 R1. To correct this issue, the applicability of CIP-004-5 R2.3, R2.5, and R6.3 should be modified to remove the references to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R3.1, R3.2, R4 (and sub parts), R5 (and sub parts), R6.1, R7.1, and R7.2 will likely need to be split into multiple requirements to properly address the applicability scope differences. (5) Electronic access: The applicability of revocation requirements in CIP-004-5 R7.1 for Interactive Remote Access should be modified to exclude "dial-up connectivity." This requirement will likely need to be split into multiple requirements to properly address the applicability scope differences. (6) Information access: There are inconsistencies between CIP-004-5 and CIP-011-1 with respect to the applicability of BES Cyber System Information requirements. CIP-004-5 R2.3, R6.1, R6.4, R6.7 and R7.3 should be modified to match the applicability of CIP-011-1. Additionally, if a change that Oncor in proposing to CIP-011-1 R1 and R2 is accepted, then there will be further inconsistency between CIP-004-5 and CIP-011-1 that should be reconciled. In its comments to CIP-011-1, Oncor proposes that the applicability 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 CIP

version 4. If Oncor's proposal for CIP-011-1 is adopted, it will become necessary to adjust the CIP-004-5 requirements for information access accordingly. To correct this issue, the applicability of CIP-004-5 R2.6, R6.4, R6.7 and R7.3 should be modified to remove the reference to "dial-up connectivity" in the applicability column. The requirements for CIP-004-5 R6.1 will likely need to be split into multiple requirements to properly address the applicability scope differences. R7 REQUIREMENT COMMENTS: The requirement language for CIP-004-5 R7.2 should be modified as follows: "For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the DETERMINATION THAT ACCESS IS NO LONGER NECESSARY." This provides clarity regarding the timing of the access revocation. 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.

Yes

No

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.

R2 APPLICABILITY COMMENTS: (1) The definition of "Interactive Remote Access" or applicability of CIP-005-5 R2.1, R2.2 and R2.3 should be adjusted to reflect the exclusion of serially connected/non-routable/non-network connected devices. There is minimal reliability benefit and significant cost associated with applying the CIP-005-5 R2 requirements to all serially connected/non-routable/non-network connected devices that require remote access. Authentication when establishing connectivity to these systems is covered by CIP-005-5 R1.4 and provides the required cyber security. The cleanest way to correct this issue is to adjust the definition of "Interactive Remote Access" as follows: "All user-initiated access OF BES CYBER ASSETS WITHIN AN ELECTRONIC SECURITY PERIMETER by a person that originates from a Cyber Asset that is not an Intermediate Device and not located within any of the Responsible Entity's Electronic Security Perimeter(s), whether routable or dial-up access, using a client or remote access technology. Remote access may be initiated from: 1) Cyber Assets used or owned by the Responsible Entity, 2) Cyber Assets used or owned by employees, and 3) Cyber Assets used or owned by vendors, contractors, or consultants. Interactive remote access does not include system-to-system process communications." Alternatively, the applicability of CIP-005-5 R2.1, R2.2 and R2.3 could be changed from "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity." (2) There is no mention of serially connected/non-routable/non-network connected devices in the CIP Awareness Bulletin (Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) that initiated the CIP-005-3 SAR or the Guidance for Secure interactive Remote Access that was ultimately issued after the CIP-005-3 revisions were not adopted. All discussions in these documents are in the context of IP addressable devices connected to a network that could be protected through the use of VPNs, proxy servers, etc. The current definition of "Electronic Security Perimeter" in the "Definitions of Terms Used in Version 5 CIP Cyber Security Standards" has evolved to make a delineation between devices that are connected to a network via routable protocol and those that are not. This approach is consistent with and further supports Oncor's proposal to adjust the definition of "Interactive Remote Access" to exclude serially connected/non-routable/non-network connected devices. (3) In addition, in Consideration of Comments – Cyber Security Order 706 Version 5 CIP Standards (definition of "Electronic Access Point" section), it provides the following: "The SDT has not included serial, non-routable communications within the definition of EAP (other than with respect to dialup in CIP-005 R1.4). Dedicated serial communications are intentionally left out of scope, as the SDT believes it would be inappropriate for the standards to mandate a universal perimeter or firewall type security across all entities and all serial communication situations. There is no 'firewall' capability for a RS232 cable run between two cyber assets. Without a clear security control that can be applied in most every circumstance, such a requirement would just generate TFEs." This demonstrates that the SDT considered and rejected the inclusion of serial, non-routable devices and specifically chose not to include them in the definition of "Electronic Access Point." Thus, Oncor's proposal is simply urging that the same approach be taken with respect to "Interactive Remote Access" and that it not include serially connected/non-routable/non-network connected devices. (4) Oncor further requests additional information in the guidance section that addresses what is and is not a remote access client or remote access technology.GENERAL COMMENT: Oncor supports the comments submitted by EEI in response

to this question.
No
Yes
No
R1 REQUIREMENT COMMENTS: (1) The 99.9% availability requirements associated with CIP-006-5 R1.4 and CIP-006-5 R1.6 would place an undue burden on the Registered Entities to accomplish the desired availability and maintain satisfactory supporting documentation while resulting in negligible reliability improvements when applied to “Medium Impact BES Cyber Systems with External Routable Connectivity.” These requirements are particularly troublesome when considered in the context of remote switching station locations that are subject to the performance of communication channels to achieve these requirements. One could assume that to reliably achieve a 99.9% availability of Physical Security Perimeter monitoring/control, it would be necessary to post a guard (or have someone on-site) 24x7x365. For these reasons Oncor proposes to limit the applicability of these requirements to High Impact BES Cyber Systems. As CIP-006-5 R1.4 and R1.6 apply to “Medium Impact BES Cyber Systems with External Routable Connectivity,” the required availability should be reduced to a more reasonable percentage (99% or less) to accommodate potential communication channel outages. (2) CIP-006-5 R1.5 should be modified as follows to clarify what type of activity is being monitored and ensure that the 15-minute clock does not start until the message reaches the monitoring location: “Issue an alarm or alert in response to detected unauthorized ACCESS into a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection AT THE MONITORING LOCATION.” CIP-006-5 R1.4 and 1.6 address the availability requirements of the access and monitoring systems, thus CIP-006-5 R1.5 should only address how the detection is handled after notice is received at the monitoring location. (3) CIP-006-5 R1.7 should be modified as follows to clarify that the 15-minute clock starts after unauthorized physical access is detected: “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the DETECTED unauthorized physical access.” R2 REQUIREMENT COMMENTS: The wording of CIP-006-5 R2.1 should be simplified by shifting the focus from visitors to individuals. Proposed wording for CIP-006-5 R2.1: “Require continuous escorted access of INDIVIDUALS NOT AUTHORIZED FOR UNESCORTED PHYSICAL ACCESS within each Physical Security Perimeter, except during CIP Exceptional Circumstances.” R3 APPLICABILITY AND REQUIREMENT COMMENTS: The category of “locally mounted hardware or devices at the Physical Security Perimeter” requires additional detail, or it should be removed. This concept originates within the “Physical Access Control System” definition (where locally mounted hardware is exempt) and extends into the CIP-006 requirements. The term “locally mounted hardware or devices at the Physical Security Perimeter” is overly broad and could arguably include hardware and devices that have little or no impact on security. Likewise, documenting outages for “locally mounted hardware” could require significant resources and yet provide minimal, if any, security benefit. Therefore, Oncor proposes that “locally mounted security devices” be substituted in place of “locally mounted hardware or devices.” 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.
Yes
No
No
No
No
R2 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. R2 REQUIREMENT COMMENTS: The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. R3 APPLICABILITY COMMENTS: (1) Oncor proposes that

the applicability of CIP-007-5 R3.1, R3.2 and R3.3 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity." This will minimize the application of these requirements to devices that are not susceptible to malicious code because they are not connected to a network with external routable connectivity. (2) The applicability of CIP-007-5 R3.3 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity" in recognition of the need for external connectivity to accomplish the 35-day update cycle. Registered Entities may be encouraged to remove malicious code protections that use signatures or patterns from medium impact systems without external connectivity if they are required to visit the site every 35 days to update signatures or patterns. R4 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R4.1 and R4.4 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity." This will minimize the application of these requirements to devices that are not capable of the detecting/logging requirements in CIP-007-5 R4.1, thus reducing documentation requirements that have no impact on security. R4 REQUIREMENT COMMENTS: (1) In addition to the applicability changes, Oncor requests that the "Requirement" language of CIP-007-5 R4.1 be revised to match the "Measures" language as follows: "Log events OF WHICH THE BES CYBER SYSTEM IS CAPABLE OF DETECTING AND, FOR GENERATED EVENTS THE BES CYBER SYSTEM IS CONFIGURED TO LOG for identification of and after the fact investigations of…." (2) A qualifier should be added to the end of CIP-007-5 R4.1.4 to indicate that malicious activity should be detected and logged "as required in the cyber security incident response 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.
R5 APPLICABILITY COMMENTS: Oncor proposes that the applicability of CIP-007-5 R5.1 and R5.4 to "Medium Impact BES Cyber Systems" should be limited to "Medium Impact BES Cyber Systems with External Routable Connectivity or Dial-up Connectivity." This will create consistency with the applicability of CIP-004-5 R6.2 and correctly captures the asset classifications for which authentication would provide a reliability benefit. R5 REQUIREMENT COMMENTS: (1) CIP-007-5 R5.2 and R5.3 are redundant to CIP-004-5 R6 and should be removed. Authorized access is addressed in CIP-004-5. (2) The requirement language of CIP-007-5 R5.4 should be modified as follows: "Change KNOWN default passwords, where technically feasible, unless the default password is unique to the device of instance of the application, on Cyber Assets." This will prevent Registered Entities from being held responsible for accounts that are unknown to them. GENERAL COMMENT: Oncor supports the comments submitted by EEI in response to this question.
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.
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
No
Yes
No
No
R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Consider removing R2.10, it is difficult to determine the intention of this requirement. It does not add anything that is not covered in 2.2 through 2.9 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based R 4.3 –We believe that the term “criteria” should be left out of the requirement. Reviewing PRAs is a highly subjective process that is handled on a case by case basis, and we believe that only a process that helps drive decisions should be included here.
R 6.6 - Remove Measure “2. A summary description of privileges associated with each group or role;“ R 7.2 –In reassignments or transfers knowledge transfer can take extended period of time (some positions that are recently vacated also are not immediately filled when transfer/reassignment is completed). Stipulations should be present to allow for this knowledge transfer to ensure that access is not revoked before it is truly not needed any longer. The change rationale does not match part 7.2. As stated above, the requirement in the table currently reflects the need to cut access immediately as of the transfer, rather than allowing for proper transition plans to be executed. Measures for 7.2 contain numbered list. The opening line should read ‘Evidence must include’. Or the list should be changed to a bulleted list.
No
No
Part 5.1 remove the word “all” or be specific to scope. Define what is meant by “user access”. Provide better examples for measures in order to provide guidance for intention of the requirement. Reword requirement to “Enforce authentication of interactive user access to Applicable BES Cyber Systems and associated Cyber Assets, where technically feasible.” or change to require authentication of accounts. R1.1 – Requirements mention Cyber assets that are not in the applicability column R1.2 Add external routable verbiage under applicability of last item R1.3 & 1.5 Access points for assets needs to be clarified. Is it ESP? R1.4 Add associated Cyber assets in applicability column R1.5 The Measures are prescribing an Intrusion Detection System, however such system is not prescribed in a requirement. The references to an IDS should be removed or it should mention that other methods are available. Other systems and tools can be used to detect malicious communication other than an IDS.
We will wait for IRC comments
No
No
Yes
R1.8 – Please add verbiage to include exit as well as entrance. There also needs to be an exception to include emergency exit such as fire drill (CIP Exceptional Circumstance) Evidence retention – Is it evidence or data that should be kept for 90 daysit? One may be able to show evidence of logs but not be able to produce the actual data itself R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement R3.2 says to retain records for 12 months. In order to meet the 3 year requirement could we get clarity on producing evidence of compliance vs the actual data?
No
No
No
No
No

R1 - Instead of class of cyber asset, use verbiage from CIP 10 Requirements need to address justification for ports & services that are enabled R2 Please provide clarity on what constitutes a security patch Please provide clarity on what it means for a cyber asset to be updateable R2.2 can a control system vendor be referenced as the source for the 30 day timeline even if the patch originates from a technology vendor? Please provide clarity on what “applicability” means 2.3 “the vulnerabilities within exposed by each security patch” insinuates that the security patches create vulnerabilities R3 R3 and R4 one states malicious code and the other states malicious software. Suggest changing to malicious code for consistency. Part 4.1.4 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2.1 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2 remove “real-time”. Is real-time when the event is received by a tool or when the event occurred on a cyber asset. Some events may only be processed by a tool on a daily basis (batch). Part 4.3 standardize with CIP-006 R1.6 in regards to availability and keeping records for outages. Is the requirement in regards to the security monitoring logging capability or in regards to a cyber asset not logging? R4.4 should be bullets rather than numbers Part 4.5 should only pertain to where automated processes and alerting are not possible. Evidence retention – Is it evidence or data that should be kept for 90 daysit? One may be able to show evidence of logs but not be able to produce the actual data itself
5.6 does not match he other R5 sections in the Applicability column. “Medium Impact BES Cyber Systems at Control Centers with External Routable Connectivity" R5 & R6, remove attestation as a measure, instead “provide procedure” R5.6 Periodically spelled incorrectly as “Periodicity”
Individual
Frank Dessuit
NIPSCO
Yes
Yes
Yes
No
Yes
Yes
No
R2: Change the measure to indicate “Cyber Security policies” instead of “Security Controls” to be consistent with the requirement. R4: NERC should clarify whether modifications to this standard require current personnel with access to undergo another background check, or whether they be grandfathered in. Setting a hard line of when employees “fail” a PRA is difficult, as it may determine on what role the individual is performing. It might even be more difficult to have “fails” defined for each role within the organization. The registered entity should be permitted to establish criteria that includes the entity using judgmental decision making. 4.2.3 NERC should clarify whether this applies to distance learning (e.g., online universities). 4.2. NERC should clarify whether this requirement applies to the location a contractor has been working at or his company headquarters. 4.3 Requirements will need to be negotiated with applicable unions and labor agreements. 5.2 NERC should clarify whether data retention of the current and previous personnel risk assessment records requires a responsible entity to maintain 14 years of background history.
R7: NERC should provide a precise definition of “Termination Actions”. 7.5 This requirement is overly and unduly burdensome because physical and interactive remote access has already been removed. With these accesses being removed entities should be able to change shared account passwords on their normal schedules. 7.2 There are times when a transferred employee still needs access due to transitional responsibilities; therefore, access will be required beyond the next calendar day. The requirement should be changed to state that the employee’s access will be removed at the end of the transitional period.
Yes
Yes
1.1, “Associated Protected Cyber Assets” should be removed from the requirement or added to the Applicable BES Cyber Systems and Associated Cyber Assets column.

No
Yes
Yes
R1.6 – NERC should resolve inconsistencies in the measures and the requirements.
Yes
Yes
Yes
No
Yes
R4.1 – No TFE's are allowed on this requirement. NIPSCO is concerned that not all devices can satisfy this requirement. R2.2 and 2.3 – Change the applicability to 35 calendar days to allow for a once a month frequency with slight flexibility to account for months with 31 days or for beginning or ending of months on weekends
Individual
Andrew Gallo
City of Austin dba Austin Energy
Yes
No
No
No
No
No
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Yes
No
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
Please see the comments submitted by the Texas Reliability Entity NERC Standards Review Subcommittee to which Austin Energy has subscribed.
No
Yes
No
The Requirement 1.7 table states: "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access." Austin Energy believes the following language better reflects the purpose of the Standard: "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the Physical Security Plan within 15 minutes of the unauthorized physical access." Additionally, please see the comments submitted by the Texas Regional Entity's NERC Standards Review Subcommittee, to which Austin Energy has subscribed.
Yes
No
No
No
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.
Individual
Steve Karolek
Wisconsin Electric Power Company
No
No
No
No
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. (2) Table R1 Part 1.1 simplify wording from "conveys ongoing reinforcements" to "reinforces". (3) Table R4 Part 4.2 strike "at least" from the phrase "covering at least all locations" since all should be all and there is nothing more for it to be least of. Also, add the word "consecutive" to the six months requirement and specify "or" between resided or employed or attended school. (4) Table R4 Part 4.3 and Part 4.4 needs clarification that either a process or a list of criteria is sufficient for compliance. (5) Table R5 Part 5.1 delete the word "granted" from the phrase as it is redundant and potentially misleading. (6) Table R5 Part 5.1, remove the adjective "authorized" where it appears in the phrases "authorized electronic" and "authorized unescorted" as this adds confusion. (7) The first paragraph of guidelines and technical basis for R4 and R5 is a single sentence which runs on for 115 words. Please break this paragraph into discrete thoughts with shorter and easier to understand sentences.
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. (2) Table R6 Part 6.5 Measures column, please apply consistency of word order to "Dated document of verification..." and "Documentation of dated verification..." We have no preference for which order as long as there is consistency applied. (3) Table R7 Part 7.1 The current language and application guidelines fail to account for a few out-of-service transactions in which entities will not be able to meet the standard. For instance, an individual might be temporarily suspended while a performance or a misconduct investigation occurs. Perhaps ten days later, the individual is terminated but the effective date of the termination is the last day worked. The compliance personnel may be notified and act promptly on the date that the employer determines the individual should be terminated, but the records will indicate that compliance personnel acted ten days late. Consequently, we recommend a change from the wording "For termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action and complete the revocation within 24 hours after the effective date and time of the termination action" to "For termination actions, initiate the process to revoke the individual's unescorted physical access and Interactive Remote Access when the entity determines that the individual should be terminated and complete the revocation within 24 hours after the effective date and time of the such determination". (4) VSLs for R7, Moderate. The sample violations should be moved down the scale one notch each. A single failure to revoke access for one individual should be in the lower VSL column, not the moderate VSL column. This also makes it consistent with the failure to act on a timely basis in the revocation of access to BES Cyber Information for a single individual.
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications (1) Table R1 Part 1.5 Measures column says "may include but is

not limited to". This is not consistent with the use of numbered lists separated by "and" which require inclusion of all list items. This wording needs to be clarified to indicate whether this is an "and" requirement which must include all items or an "or" requirement which may include but is not limited to these example items.
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EEI.
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Table R1 Part 1.5, simplify the wording "...unauthorized circumvention of a physical access control..." to "...unauthorized access..." (2) Table R1 Part 1.7 we suggest the action be related to detection. "...within 15 minutes of detecting unauthorized physical access". (3) VSL table R2 Moderate, delete "on a daily basis" which adds nothing to the meaning and, in fact, may lead to confusion in compliance. For example, what would a compliant record look like for a visitor whose visit lapsed from one calendar day into the next? (4) In the guidelines and technical basis for R1, delete any reference to the maximum size (96 square inches) of an opening. With the end of "six-wall perimeters", and the establishment of the requirement to enforce access control for the physical border surrounding locations, the number is meaningless.
No
No
No
No
No
Wisconsin Electric Power Company supports EEI Member Consensus comments with the following additions/exceptions/clarifications: (1) Table R1 Part 1.1 the listing of listening ports and services appears to be overlap or duplication with the baseline configuration requirements of CIP-010 and Wisconsin Electric is concerned about potential "double jeopardy" issues if something is missed on a list. If we have to retain the list for CIP-010 it should not also be required for CIP-007.
Wisconsin Electric Power Company supports EEI Member Consensus comments as submitted by EEI.
Individual
Kathleen Goodman
ISO New England Inc.
No
No
Yes
No
Yes
Yes
No
Recommend removing “, but not limited to,” from R1 Part 1.1 Measure since the Measures are only guidance Recommend removing “potential” from R2 Part 2.7 since an incident is determined to be real or potential during the follow up investigation. Request additional clarification on R2 Part 2.10 in the Application Guidelines. From the CIP-004-5 Table R2 - Cyber Security Training Program, the use of the terms interconnectivity and interoperability with regard to FERC Order No. 706 needs to be clarified to make the differences and applications of the terms understood. Request clarification on R4 Part 4.2 since it is not clear if the numbers should be read as “and” plus does the six months apply to all of the numbers? Prior versions of R4 Part 4.3 had exclusions for laws or collective bargaining agreements. Please add the exclusions or explain why the exclusions were dropped. Recommend different VSL thresholds for R3. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations. Recommend different VSL thresholds for R5. Differentiating by individuals is bad for large organizations. Differentiating by percentage of associated is staff is bad for small organizations.
Request a more clearly worded R6 Part 6.4. The intent appears to be authorizing (electronic/physical)

access to BES Cyber Systems Information. Request additional clarification in this Requirement and Application Guidelines. Note that Requirement 6.1.3 also uses “physical and electronic locations.” In R7 Part 7.4, recommend changing “Requirements R7.1 and R7.3” to “Requirement R7 Parts 7.1 and 7.3.” In the corresponding Measure, recommend changing “removal” to “revoke” for consistency with the Requirement. In some systems removal results in removing all corresponding records which makes it hard to provide the proper records to the auditor. Recommend updating the R7’s Violation Risk Factor in the Table of Compliance Elements. That VRF is “medium” while the Requirements and Measures show R7 as “low”.
No
No
Recommend removing “, but is not limited to, ” from R1 Part 1.1 since the Measure’s scope already includes all of the possible Cyber Assets Measures should not dictate Requirements. If correct, then how can CIP-005 R1 Part 1.5’s Measure specify “intrusion detection system” when the Requirement does not specify a technology? Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from “intrusion detection system” to “detection system” Request for clarification on how the math for R1 is done in the VRF/VSLs.
Request clarification on R2 Part 2.1 – can the Intermediate Device be on the ESP? Can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from “Factors must be at least two of the three following categories” to “Multi-factor include, but are not limited to” which allows future technology without a Standards update.
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are tested every 36 months.
Yes
No
No
No
No
For R2, request clarification if the SDT’s intent is that the following timeline will be compliant or not. 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from “(1) immediate detection” to “(1) real time detection” to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect “deny by default” firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? The wording in the Measures column does not reflect what the Requirement is stipulating. Recommend removing “malicious” from R4 Part 4.1.4 since “malicious” is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe. Recommend that the number of assets should be another differentiator for R3’s Low – Moderate – High – Severe. Recommend that the difference between R4’s Low – Medium – High – Severe should be the number of assets with two weeks throughout Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low - Medium - High - Severe.
Request clarification of R5 Part 5.7. Does the technical feasibility apply to both “the number of

unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful log in attempts" or only the "authentication attempts?"
Group
SMUD & BANC
Joe Tarantino
No
No
Part 6.5 requires that the entity verify each calendar quarter that individuals provisioned for authorized electronic access or authorized electronic access or authorized unescorted physical access have associated authorization records. The measures include "Documentation of the dated verification between a list of individuals who have been authorized for access …. And a list of individuals provisioned for access…". The reason a review should be necessary is the possibility that there is an error that needs to be corrected. The evidence in the Measures requires perfection on the part of the entity because it requires a dated verification between a list of individuals who have been authorized for access and a list of individuals provisioned for access. The event that a mismatch is discovered should give the entity the opportunity to fix the problem rather than be a violation. As worded, any mismatch discovered would result in a violation. Therefore, the standard requires perfection – anything less is a violation. It is suggested that the Measures be changed to simply prove that the review was completed while leaving the results of the verification out of the Measure. Parts 6.6 and 6.7 - Similar to our comment on Part 6.5, the Measures should only require verification that the entity performed the verification while leaving the results of the verification out of the Measure. This is especially true in the item number 4 in the measures: "Dated evidence showing verification of the privileges for the group are authorized…". Suggest wording in the measures that states, "Evidence … that proves the entity performed the annual verification." This reflects our previous comments on this issue. It appears that the standard is requiring perfection. If so, what is the point of the quarterly review? As worded, it looks like the purpose of the quarterly review is to find violations rather than give the entity an opportunity to fix the problem. Part 7.1 provides for limited revocation (remote access and physical access) for all terminations in 24 hours while Part 7.2 requires that all electronic access not needed is revoked by the end of the next calendar day for reassignments and transfers. Part 7.2 is inconsistent with the Rationale in 7.4, which states "Some cases may take more time to coordinate access revocation on individual Cyber Assets and applications without affecting reliability." If this statement is true for Part 7.4, then it is also true for Part 7.2 because in both cases, individual account access is revoked in both cases. The transfer or reassignment presents a special problem. If physical access needs for the new position and the old position are the same, but cyber access needs between the two positions are different, then one cannot use the mechanism of fast revocation of physical access and remote access to prevent the employee from accessing accounts he/she previously had access to in the old position, but has no need to access in the new position. While this logically leads to the conclusion that all cyber access needs to be removed very quickly, this conclusion conflicts with the Rationale that entities need time to comply. The same reasons that would have made it difficult for entities to remove all cyber access for terminations in a very short timeframe are the same reasons that would make it difficult to remove cyber access in the same timeframe for reassignments and transfers. It is suggested that entities be given a minimum of 7 days to revoke unneeded access for assignments and transfers.
No
No
No
No
Req. R1 1. SMUD appreciates the changes made by the drafting team with respect to the physical ports. The language in Draft 2 is much preferred over the language in Draft 1. However, the physical protection of all assets including physical ports is already covered in the physical security perimeter defined in CIP-006-5. SMUD's opinion is that the protection of physical ports defined in this section is

duplicative, and presents unnecessary burden to the entities. 2. The Rationale for R1 for this draft no longer includes a reference to physical ports. But requirement R1.2 concerns physical ports. The Rationale doesn't match requirement R1.2. Req. R2 1. Requirement R2.3 goes beyond the control of an entity that is reliant on a vendor to identify and provide patches for vulnerabilities. The entity's only typical options are to either install the patch or not install the patch. a. The vendor's development cycle may be the only path by which the vulnerability can be addressed. b. The entity cannot typically specify a specific timeframe in which the vulnerabilities will be addressed in the written plan that is required by R2.3 without basing its timing on the completion of the vendor's development cycle. 2. It is unnecessarily burdensome to require the entity to write a new remediation plan (or revise an existing one) for every patch because the entity generally simply installs the patch. It is suggested that a remediation plan only be required when the entity determines that it should not install the patch. This meets the intent of the Change Rationale shown in Table R2 of CIP-007-5. a. In the event the entity chooses to install the patch, documented tracking of the handling of the patch could be executed through an entity's documented procedures. In this case, there is no need for a remediation plan. The procedures the entity uses to define the workflow should be part of the Patch Management program that is already required. b. In the event the entity determines that it is too risky to install the patch, a written plan could be required to direct the entity to document what it plans to do to mitigate the vulnerability. 3. Regarding the dated plan referenced in Parts 2.3 and 2.4, it is possible that the entity's only option would be to notify the vendor and wait for a subsequent patch. In this situation, the entity will be able take steps toward final resolution, but would not be in the position to mitigate the vulnerability within any specified timeframe. The entity would be unable to specify when the vulnerability will be mitigated in the plan. Even though the entity could revise the plan to change the date the vulnerability would be mitigated, it is unnecessarily burdensome to require the entity to do so. 4. Measures on 2.4. It is appreciated that the team added the bullet items "Records of the installation of the patch"; and "Records of implementation of vendor recommended mitigations". It is still not clear that certification of installation of a patch onto a BES cyber system (for example: through a workflow) would be considered sufficient evidence. An auditor may interpret "Records of installation of the patch" to mean that records need to be kept for every machine. It is suggested that the wording be included to state that acceptable evidence would include certification by the installer that the patch was installed on the BES cyber system or BES cyber asset. Req. R4 SMUD appreciates the changes made to this section in the previous draft. In part 4.4, Measure 2 requests information about log data that is not part of the requirement. Thus, item 2 doesn't match the requirement and adds unnecessary burden for the entity. Measure 1 proves the existence of log information for 90 days. Measure 3 proves that the system is configured for 90 log retention. Taken together Measure 1 and Measure 3 prove that the system meets the requirement.
The "Summary of Changes" section includes a statement that says that requiring "the identification and management of shared account access have been removed." Requirement 5.3 states "Identify individuals who have authorized access to shared accounts". The Measure to Requirement 5.3 states includes the phrase "…listing of shared accounts and the individuals who have access to each shared account." While the Measure includes the phrase, "Evidence may include, but is not limited to,…", the example still requires identification and management of shared accounts. Requirement 5.4. The Phrase "on Cyber Assets" may add confusion. It appears that the intent of the requirement would be met (without change) if this phrase were removed. Requirement 5.5.2. "Minimum password complexity that is the lesser of three or more different types of characters (eg. uppercase alphabetic, lower case alphabetic, numeric, non-alphanumeric) or …" It is appreciated that the intent is to give maximum flexibility to the entity by leaving it to the entity to define character types. Unfortunately, there is no definition for the word "types". Instead, the language presents the types as an example: "(eg. uppercase alphabetic, lower case alphabetic, numeric, non-alphanumeric)". The ability to enforce or comply with Part 5.5 depends upon a definition of what really constitutes a character "type", or, alternatively, a different way of defining password complexity.
Group
Southern California Edison company
Nathan Smith
No
No
No

No
No
No
No
SCE Comments to CIP-004-5 -R3.1: We suggest revising the requirement to say “documentation of the training specified, for their role, in CIP-004-5,..” -R3.2: We suggest revising the requirement to say “documentation of the training specified, for their role, in CIP-004-5,..”
SCE comments to CIP-004-5 -R6.1.3: Please clarify that if a person has BES Cyber System Information on their work computer or in their work station, authorized access to the computer and workstation is not required pursuant to R6.1. -R6.1.3: Please clarify if access beyond the workstation is applicable to R6.1? -R6.4: Please revise as follows: “…is stored by the Responsible Entity that the Responsible Entity determines are necessary for performing assigned work functions, except for CIP Exceptional Circumstances, pursuant to the Responsible Entity’s BES Cyber System information protection program.” -R7.1 and R7.5: These requirements appear inconsistent with each other. Please clarify R7.5 is only applicable to shared user accounts. -R7.4: Please revise as follows: “…within 30 calendar days of the effective date of the termination action. The registered entity will ensure that in the case of employee terminations, all information copied from its repositories by a terminated person is recovered or rendered useless within 30 days of that person’s termination, pursuant to the Responsible Entity’s BES Cyber System information protection program.” -R7.5: Please revise as follows: “For termination actions, reassignments, or transfers, change passwords for shared account(s) known to the user within 30 calendar days of the completion of the termination action, reassignment, or transfer of the user.”
No
Yes
SCE Comments to CIP-005-5 -R1.1: The phrase “associated protected cyber assets” should be relocated to the applicability section. - R1.3: Tracking the rationale for granting access permissions for sixty-thousand ports is burdensome. We suggest tracking the rationale for granting access permissions based upon a class of assets or the type of access required; or replacing the word “rationale” with the word “criteria”. Also please define the term “access permissions”. -R1.5: Many of the assets that fall into Medium Impact cannot accommodate an automated method for detecting malicious software. We suggest removing Medium Impact assets from the applicability.
Yes
Yes
Yes
SCE Comments to CIP-006-5 -R1.4: Please revise the requirement to the following: “…for unauthorized circumvention of a physical access control into a Physical Security Perimeter. The 99% availability includes times when back-up monitoring systems are deployed.” -R1.5: Please revise to the following: “…alert in response to detected unauthorized physical access of a Physical Security Perimeter…” Violation Severity Level for R1.9: Please remove the “did not retain physical access logs for 45 days” scope from the Severe category and move it to the Low or Medium category, as not retaining a log itself will not degrade the functionality of the BES.
No
No
No
No
No
SCE Comments to CIP-007-5 -R1.1: Please revise as follows: “…and where technically feasible, enable only required logical network accessible ports…” -R1.2: Please remove the word “unnecessary” from the requirements globally and replace it with “not required”. -R3.1: Please revise the Measures section as follows: “…Entity’s performance of these processes (e.g., through traditional antivirus, system hardening, non-software policies, etc.).”
SCE Comments to CIP-007-5 -R5.3: It is unclear what protection is gained by maintaining a list of persons that have access to shared accounts on Cyber Assets with no external routable protocol.

Please limit the applicability to High Impact Cyber Systems and Medium Impact BES Cyber Systems with external routable connectivity. -R5.7 Please clarify that printers and multifunction machines are out of scope. Please also revise the applicability section to remove “Associated Protected Cyber Assets” from the applicability section as this term could be applied to assets that do not have BES Cyber System Information, and have little impact upon the BES.
Individual
Scott Miller
MEAG Power
Yes
Yes
Yes
Yes
Yes
Yes
No
In R2 Part 2.10, “training content on risks associated” – it’s not clear what is required. Awareness and other training (i.e. part 2.4) would cover this area in general; we don’t believe that this specific training module is required.
CIP 004-5 R7 (Table R7 - Part 7.1) requires that the revocation process be completed within 24 hours for termination actions involving employees with access to certain Medium Impact BES Cyber Systems. While MEAG Power agrees that this 24 hour termination period should be the standard for employees that have been terminated and previously having access to High Impact BES Cyber Systems, the standard should allow a more reasonable response time (suggested 48 hours) for employees having access to Medium Impact BES Cyber Systems and associated protected information.
Yes
Yes
No
Yes
Yes
R1 (Parts 1.4 and 1.6) mentions that Physical Access Control Systems should have a “99.9% availability” – which so– but perhaps this 99.9% needs clarifying under CIP 006 R1 at this time. In R1, the references to 99.9% availability are not clear. There is no guidance as to how this can be measured. Also, how is one to know unauthorized circumvention? This could be interpreted to equate to a violation if there is a substation circuit downtime at any given site that is >9 hours in any one year. It is common for telco circuits to go down 1-3 times a year - probably averaging somewhere around 24-48 hours per circuit downtime event – therefore, if circuit downtime contributes against the 99.9%, there will be multiple violations at multiple sites per year. It could be argued that the centralized physical access computer system should have a 99.9% availability – which will require utilities to have primary and backup server systems in place to meet the 99.9% availability of the overall service. R1 needs to be clarified. R 1.4: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. R1.6: We suggest specifying that planned maintenance be excluded and apply the 99.9% requirement only to unplanned outages. The proposed language for CIP 006-5 R1 (Table R1 - Part 1.3) stipulates for High Impact BES Cyber Systems the requirement that “Where technically feasible, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters….”. Currently, many in the industry question if two different control systems are required. It would be recommended to clarify in the requirement that two authentication methods using the same control system are compliant (for example, badge/thumbprint).
Yes
Yes

Yes
Yes
Yes
Individual
Heather Laws
Portland General Electric
Yes
Yes
Yes
Yes
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.
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.
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.
No
No
No
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
Yes
No
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.
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.
Group
Progress Energy
Jim Eckelkamp
No
No
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= Original R1.1: A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. Proposed R1.1: A security awareness program that, at least once each calendar quarter, conveys ongoing reinforcement of cyber security practices for the Responsible Entity's personnel who have unescorted authorized electronic or authorized unescorted physical access to BES Cyber Systems. Rationale: Unescorted Cyber Access category should be introduced to allow for more effective interaction with vendor support services. Much of the CIP-004 personnel risk assessment requires extensive dependencies on supporting evidence which is not available under standard support contracts which require 24*7 staffing. There currently exists tools to monitor interaction of remote vendor support and limiting requirements to those having unescorted access within the CIP requirements will allow more effective focus of resources R2= This only applies to personnel who have escort duties; and only applies to people who have unescorted access; not access to media. Need to add whether they need training for each of the three bullets. Insert "unescorted" into "authorized unescorted electronic" references. This allows entities to focus on unauthorized access rather while allowing for vendor support services. R2.2 – Requirements, Rewording Original: Training content on the cyber security policies protecting the Responsible Entity's BES Cyber Systems. Proposed: Training content on the cyber security policies protecting applicable cyber assets. Rationale: This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). R2.3 – Requirements, Rewording Original: Training content on the physical access controls protecting the Responsible Entity's BES Cyber Systems. Proposed: Training content on the physical access controls protecting applicable cyber assets. Rationale: This allows for training to be targeted addressing applicable cyber assets (to include BES Cyber Assets where applicable). R3= R3.1 – change reference from "physical access to BES Cyber Systems" to "physical access to applicable cyber assets" to ensure training adequately covers relevant and applicable cyber assets. R4= R4.1 – Requirements, Rewording Original: An initial personnel risk assessment ("PRA") that includes identify verification. Proposed: Program content on an initial personnel risk assessment that includes identity verification. Rationale: This requirement should address the contents of a supporting program rather than individual artifacts of evidence. R4.2 – Requirements, Rewording Original: Seven year criminal history

records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: Proposed: Seven year criminal history records check including current residence, regardless of duration, and covering all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six consecutive months or more: Rationale: Two changes have been made. “At least” was dropped in front of “all” as it was redundant with “at least all.” Also, “consecutive” was added in the middle of “six months” to provide greater clarity in terms of what the criteria is. R5= R5.1 – Requirements, Rewording Original: Have a personnel risk assessment performed as specified in CIP-004-5, Requirement R4 prior to being granted authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Proposed: Have a personnel risk assessment as specified in CIP-004-5, Requirement R4 prior to gaining authorized electronic or authorized unescorted physical access, except for CIP Exceptional Circumstances. Subsequent authorizations, within the life-time of PRA events, do not require repeating the background check. Rationale: while not perfect, it was determined that “gaining” would be better terminology than “granting.” The additional language regarding not repeating this requirement provides clarity that this process is to be conducted once for any/all authorized access and is not subject to additional PRAs as additional access requirements are identified. R5.1 – Measures, Rewording (First bullet) Original: Dated records showing that personnel risk assessments were completed before authorized electronic or authorized unescorted physical access was authorized; or Proposed: Records showing that personnel risk assessments were performed before authorized unescorted electronic or authorized unescorted physical access was gained. Rationale: There is repetition of “authorized” within this measure which is confusing. By replacing the last word with provisioned, the event is better captured to ensure compliance with the PRA requirement. R5.2 – Measures, Rewording Original: Evidence may include, but is not limited to, current and previous personnel risk assessment records. Proposed: Evidence may include, but is not limited to, current personnel risk assessment records. Rationale: Given the 7 year cycle, ensuring that the current records are in place should satisfy this requirement. Addition of previous PRA records only adds to the archival length to a period of (up to) 14 years without any benefit to security.
R6= R6.1 Applicability should remove references to dial-up connectivity Comment: Measure should add ‘unescorted’ in front of electronic access. Rationale: this provides more effective applicable cyber assets to enact these requirements. Adding unescorted access allows for vendor support requirements without elevating this into ‘authorized electronic access’ category. R6.2 Requirement Rewording Original: The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. Proposed: The individual(s) designated in Part 6.1 shall authorize electronic access that the Responsible Entity determines is appropriate. Rational: assessing the appropriateness of access permissions is more effective then assessing ‘necessary.’ R6.3 Requirement Rewording Applicability should remove references to dial-up connectivity Original: The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances. Proposed: The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the Responsible Entity determines is appropriate, except for CIP Exceptional Circumstances. Rationale: Providing a scope of PSP access frames this requirement within the context of the CIP scope, focusing on defined PSP access. R6.6 Requirement Rewording Original: For electronic access, verify at least once each calendar year, not to exceed 15 calendar months between verifications, that all user accounts, user account groups, or user role categories, and their specific associated privileges are correct and are those that the Responsible Entity determines necessary for performing assigned work functions. Proposed: For electronic access, verify at least once each calendar year, or not to exceed 15 calendar months between verifications, that BES Cyber System access privileges are appropriate for the individual(s) or role(s) responsibilities. Rationale: The current language provides too prescriptive a list of evidence in support of this requirement. By eliminating “all,” identifying BES Cyber System access privileges will frame the context of this requirement effectively. Focusing on ensuring the privileges are appropriate vs. “correct,” allows for assessing the privileges. R6.6 Measures – This should be a bulleted list to support an “or” assessment of the evidence. R6.7 Measures – The numbered list should be a bulleted list to support an “or” assessment of the evidence. a. Last bullet – Rewrite i. Original – Dated evidence showing a verification of the authorizations and any privileges were confirmed correct and the minimum necessary for performing assigned work functions. ii. Proposed – Evidence showing a

verification of the authorization and any permissions were confirmed. iii. Rationale – The edits provide a greater focus on the root concerns to address the Requirement. R7= R7.1 – Requirement Rewrite Original: For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the termination action, and complete the revocation within 24 hours after the effective date and time of the termination action. Proposed: For all termination actions, initiate the process to revoke the individual's unescorted physical access and interactive Remote Access upon the effective date and time of the communication of the termination action, and complete the revocation within 24 hours after the effective date and time of the communication of the termination action. Rationale: By identifying the time the termination action is communicated, concerns regarding notification of terminations which are pre-dated or retro-active can be alleviated by using the communication time as the trigger event. R7.1 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence. R7.2 – Requirements Rewrite Original: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the reassignment or transfer. Proposed: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination that access is no longer necessary. Rationale: The rewording provides greater support and recognition that this process can take place until all legacy access is no longer needed, within a transition period that can take place indefinitely. By assigning the response time to the determination event, deadlines are aligned more effectively. R7.2 – Measure should show a bulleted list to reflect the "or" approach to supporting evidence.
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= R1.1: Applicability Comment: Add Associated Protected Cyber Assets with External Routable Connectivity Rationale: This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. R1.2 Applicability Comment: Add Associated Protected Cyber Assets with External Routable Connectivity Rationale: This addition aligns with the requirement, in which associated Protected Cyber Assets are also required to reside within a defined ESP. R1.4 Comment: This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. Propose: adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. Rationale: This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. R1.5 Measures – there should be bullets (rather than numbers) identifying 'or' instances.
Progress Energy agrees with EEI comments with the modified and additional comments below: 1. R2.1, 2.2, 2.3 Requirements – Proposed Change Original: Utilize encryption for all Interactive Remote Access sessions that terminate at an Intermediate Device in order to protect the confidentiality and integrity of each Interactive Remote Access session. Proposed: Utilize encryption for all routable Interactive Remote Access sessions that terminate at an Intermediate Device. Rationale: The addition of 'routable' in front of Interactive Remote Access sessions provides a clear filter that aligns with the Interactive Remote Access concept.
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= CIP-006-5 R1.4 currently states: Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized circumvention of a physical access control into a Physical Security Perimeter 1. Strike out "(with 99.9% availability)" and instead add language such as, "Establish a documented process to implement compensating measures for loss of specific functions of the Physical Access Control System". For example the loss of monitoring functionality of the PACS may be compensated by roving patrols physically monitoring PSPs or if electronic logging capability is lost manual logging can be implemented. 2. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points to the PSP. Revised language R1.4 would read: Define and implement controls that monitor physical

access points of the Physical Security Perimeter for unauthorized physical access into a Physical Security Perimeter. Establish a documented process to implement compensating measures in the event the physical access control system is non functional Rationale for change to R1.4: 1. Attempting to impose a requirement to have the physical access control system available 99.9% is not realistic or possible given some of the environments where they are being implemented (e.g., substations, a variety of types of bldgs at generation sites). It does not take into consideration possible network outages of the WAN (which entities have no control over), does not take into consideration remote locations with infrequent use (it is possible for a alarm contact to go bad with no indication of such unless one was continuously testing alarms) or the difficulty in tracking the various types of outages (no defined formula for determining the 99.9% availability). Furthermore, it does not allow entities to implement compensating measures as a means to remain compliant in the event the system is not available. The availability should be addressed by a robust maintenance program that allows for broken equipment to be found, recorded and mitigated in a timely manner without recording violations. 2. The requirement as it is written seems to imply entities would need to employ some type of interior motion detection within the PSP that would alert if physical access controls were circumvented. This seems to increase scope of the original monitoring requirement when alarms and alerts were limited to physical access points. Implementing interior motion sensors within PSPs throughout the various generation/transmission sites would provide little or no return on investment, as existing physical security controls (e.g., perimeter fencing, card access) should be sufficient based on low probability that a cyber attack will be initiated at the device level. There are no known physical security threats against cyber assets that would warrant such prescribed language. In addition, various types of interior motion detection sensors (e.g., interior microwave sensors, passive infrared, and proximity sensors) are not full proof and all are prone to nuisance alarms. Nuisance alarms vary based on type, but can be triggered by objects being moved by air currents generated by heating, ventilation, and air conditioning (HVAC) systems or fans and fluorescent lighting, interference from various electromagnetic fields, small/large insects, change in temperature, vibrations, dust, etc. CIP-006-5 R1.5 currently states: Upon detection of an unauthorized circumvention of a physical access control into a Physical Security Perimeter notification to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. 1. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points to the PSP. Revised language for R1.5 would read: Issue an alarm or alert in response to detected unauthorized physical access at all access points to a Physical Security Perimeter to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. Rationale for change for R1.5: There may not be an alarm or alert of unauthorized access, but just a response. CIP-006-5 R1.6 currently states: Have controls that monitor each Physical Access Control System twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized physical access to a Physical Access Control System. 1. Strike out “(with 99.9% availability)” and instead add language such as, “Establish a documented process to implement compensating measures for loss of specific functions of the Physical Access Control System”. For example the loss of monitoring functionality of the PACS may be compensated by roving patrols physically monitoring PSPs or if electronic logging capability is lost manual logging can be implemented. 2. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points. Revised language for R1.6 would read: Have controls that monitor physical access points to the Physical Access Control System for unauthorized physical access. Rationale for change for R1.6: Refer to Rational for Change for R1.4 CIP-006-5 R1.7 currently states: Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. 1. Revise language to align with legacy language in previous version that specifies monitoring at all physical access points. Rationale for change for R1.7: There may not be an alarm or alert of unauthorized access, but just a response. Revised language for R1.7 would read: Upon detection of an unauthorized circumvention of a physical access control into a Physical Security Perimeter notification to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. R2= R2.1 – Requirements Original: Require continuous escorted access of visitors (individuals who are known or guests, and not authorized for unescorted physical access) within each Physical Security Perimeter, except during CIP Exceptional Circumstances. Proposed: Require continuous escorted access of individuals not authorized for unescorted physical access. Rationale: The additional words did not provide any greater clarity. R3= Applicability: Remove “Locally mounted hardware or devices at the physical security perimeter associated with:” Rationale:

documenting outages for locally mounted hardware is currently too vague and resource intensive with minimal security benefit. By ensuring that Physical Access Control Systems adequately document their outages, the root concern should be addressed. a. Requirement – Change Original: Document outages for physical access control, logging, and alerting systems and retain the outage records for at least 12 months. Propose: Document outages for physical access control systems and retain the outage records for at least 12 calendar months. Rationale: By focusing on the Physical Access Control Systems, satisfactory outage records should be achieved. Additional Comments: Comments: VSL – R1/High: The second paragraph on page 23 should read "The Responsible Entity does not have controls…" VSL – R1/Medium: Remove "or external dial-up connectivity. (1.2)" from the end of the second paragraph. VSL – R2 Moderate: Remove "on a daily basis," from the 1st paragraph on page 25. Application Guidelines a. Page 28 – Remove "Methods to monitor physical access include:" section as it relates to R1.4, which has been proposed for removal. b. Page 29, second paragraph – Remove. The applicability of the 96 square inch opening provides no benefit to applicability. Focusing on unauthorized circumvention of physical access control could be interpreted as monitoring for perimeter breaches outside of the current physical access points. This could lead to exhaustive monitoring tools which may still allow for unmonitored locations that result in a violation of this requirement.
No
No
No
No
No
Progress Energy agrees with EEI comments with the modified and additional comments below: R1= R1.1 Comment: Applicable BES Cyber Systems and associated Cyber Assets: Clarify how "Associated Protected Cyber Assets" is a modifier to the "High Impact BEST Cyber Systems" and "Medium Impact BES Cyber Systems with External Routable Connectivity" rather than an independent set of assets. One option is to add "and Associated Protected Cyber Assets" to each of the High and Medium categories in this requirement. a. Requirements i. Does the "where technically feasible" language imply that TFEs are required when it is not technically feasible? ii. There was discussion about how "needed" should be defined, and whether it's up to the asset owner to determine the need for a port to be accessible, or whether the auditor has the ability to decide. This issue was tabled, and there may suggested language provided. R1.2 Requirements: Discussions around whether the physical security measures already accommodate this requirement, but it was brought up that FERC specifically requires this. Measures: Suggest a clarification that these measures be implemented at the device level if that is the intent. R2= R2.1 Requirements: Original: A patch management program for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets." Proposed: A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." R2.2 Requirements: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency R3= Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. R4= R4.1 Comment: Add the term "where technically feasible" to the requirement language Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. R4.2.1 Comment: Change "detected malicious activity" to "detected cyber security event" Rationale: not all security events are malicious R4.3 Requirement Comment: Change "Activate a response to detected event…" to "Activate a response to human-detected event…" Rationale: the requirements do not distinguish between the detection of an event by a system and a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection. Requirement: Comment: Change "next calendar day" to "next business day" to accommodate off-hour staff coverage. Measures: Change "attestation" to "documentation" for clarity. 1. R4.5 Applicability Comment: Consolidate "High Impact BES Cyber Systems" and "Associated Protected Cyber Assets", by changing the wording to "High Impact BES Cyber Systems with Associated Protected Cyber Assets" Rationale: Clarifies that the logging reviews do not apply at the asset level. Requirement Comment: Change the wording to "Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…" Rationale: It

should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits. Requirement Comment: R4.5 – standard is asking for review every two weeks Propose: monthly review
Progress Energy agrees with EEI comments with modified and additional comments below R5.1 Applicability Comment: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” Rationale: Consistency with CIP-004 R6.2 R5.2: Delete requirement. Rationale: Covered by CIP-004 R6.2 R5.3 Delete requirement Rationale: Covered by CIP-004 R6 and move rationale to CIP-004 R6. R5.4 Applicability Comment: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routability or dial -up” Rationale: Consistency with CIP-004 R6.2 R5.1 Requirement Comment: Change the wording from “Change default passwords…” to “Change known default passwords…” Rationale: Manufacturers sometimes use system passwords that are not known to the entities. R5.1 Measures Comment: Remove the language from the first bullet “…when new devices are deployed” Rationale: Time frames are covered elsewhere in the Standards R5.5 Measures Comment: Change the second bullet to “Documentation of procedural controls” Rationale: Procedural controls for changing passwords are covered elsewhere R5.6 Requirement Comment: Add the language “within the capabilities of the device or operational requirements” to the beginning of the requirement. Rationale: Some vendors do not ensure correct operation of the system if certain passwords are changed. R5.6 Measures Comment: Change the second bullet to “Documentation of procedural controls” Rationale: Procedural controls for changing passwords are covered elsewhere
Individual
John Allen
City Utilities of Springfield, MO
No
No
No
No
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.
City Utilities of Springfield, Missouri 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 requirement is 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.

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 requirement is 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
No
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.
City Utilities of Springfield, Missouri agree with the comments from SPP and APPA and believe the requirement is 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
Nick Lauriat
Network & Security Technologies, Inc.
Yes
Yes
Yes
No
Yes
No
No
In Requirement R4, N&ST observes the drafting team has attempted to address numerous concerns about the difficult in systematically checking criminal history in locations not associated with actual residence (as recorded by the Social Security Administration). The fact of the matter is that requiring entities to do a criminal history check anywhere other than the addresses on file with the Social Security Administration is a faulty approach. Candidates can easily conceal criminal history by

forgetting or ignoring a county / state where arrest may have occurred (which could be quite different from the work location or location of the educational institution). N&ST recommends the drafting team not require additional documentation from the entity, but simply require the type of information (e.g., residence) likely to be available programmatically during a commercial personnel risk assessment.
In Requirement R6, N&ST observes that as written, it appears to be required that individuals be authorized for all three types of access listed in 6.1.1 through 6.1.3. Suggest rewording to say, “Designate one or more individual(s) to authorize one or more of the following types of access:” In Requirement R7.2, N&ST observes that the drafting team appears to have inadvertently made this requirement more stringent, in terms of time allowed to complete, than Requirements R7.1 and R7.3.
Yes
Yes
No
Yes
Yes
N&ST observes that CIP-006-5 articulates a number of requirements for PSPs without ever including a requirement about what needs to be inside the PSP! N&ST suggests that Requirement R1.1 be reworded to “Define operational or procedural controls to restrict physical access to only those individuals who are authorized.”
Yes
No
No
No
Yes
In Requirement R2, N&ST observes that entities are not required to commit to any specific date to either install an applicable patch or implement other vulnerability mitigation measures. If the drafting team hopes to “get ahead” of CANs in this area, CIP-007-5 cannot remain silent on this point. In Requirement R3, N&ST observes that the wording of associated Measure suggests an entity could claim compliance with nothing more than a policy advising users to exercise caution. In Requirement R4.1, N&ST believes that this is likely to be not technically feasible for all applicable systems, and believes it should be TFE eligible (like Requirement R4.2).
Individual
Brian Evans-Mongeon
Utility Services Inc
Yes
Yes
Yes
No
Yes
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. (1) R4.2 Recommend that 4.2.1 – 4.2.3 be replaced by bullets and that the “and” in 4.2.2 be replaced by an “or”. The current language would require that all three elements be met at the same location and time period, before a criminal history check would need to be done.
(1) The Violation Risk Factor stated in CIP-004-5 R7 should agree with the VRF listed in the Table of Compliance Elements.
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this

Standard.
Yes
Yes
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. Utility Services supports the comments made by MMWEC in their Comments 1, 2 and 3 for CIP-006-5.
Yes
No
Yes
No
Yes
The comments submitted for the Applicability Section 4.0 of CIP-002-5 would be applicable to this Standard. Utility Services supports the comments made by MMWEC in their Comments 1, 2 and 3 for CIP-007-5 R1, R2, R3, R4.
Utility Services supports the comments made by MMWEC CIP-007-5 R5.
Group
NCEMC
Scott Brame
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
Yes
Yes
(1) R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes
Group
Dairyland Power Cooperative

Tommy Drea
Yes
No
No
Yes
Yes
Yes
No
Please see MRO NSRF Comments.
Please see MRO NSRF Comments.
No
Yes
The CIP-005 standard does not adequately define or address security controls required for non-routable devices. There needs to be some identifiable security requirements for serial devices that communicate external to the ESP. This needs to address the full variety of connectivity situations. For instance, communications with a remote serial end point is likely to occur over an enterprise or commercial communications infrastructure. The communications network infrastructure may contain devices utilizing either IP transport or IP management access. It would be incorrect to define this communications path as “direct serial”. Is such a path considered routable? Does it require security controls? Does it matter if the remote system is protected by security controls? Consider the following items in comparison to the draft 2 “Application Guidelines” section of CIP-004-4 draft 2. This section of draft 2 states that serial connections are not considered routable—and also that devices that communication externally with serial connections are not considered Electronic Access Points. • The “Identifying Critical Cyber Assets” Security Guideline section D defines serial devices that are connected to a network device (i.e. Terminal server, or RTU concentrator) as being “routable” by virtue that they can be accessed over a routable network. • NERC Notice of Penalty (NOP) NP12-4-000 outlines a violation of CIP-005-1 R2 that appears to be related to using external terminal server solutions to critical serial devices. It seems the utility expected the direct serial cable to be the ESP boundary. Without further details, it is unclear if there is a contradiction between guidelines. If the intention of the draft 2 guideline section is to make a blanket statement on serial being excluded from any definition of routable, then these items above are in contradiction. If this point in the draft 2 guideline is only to address serial devices that cannot be routed to, the standard is severely lacking in guidance as to how to address serial communications that do not meet the criteria of “direct serial”. The definition of a “Direct serial, non-routable” connection should be further defined. Distinctions should be made about other situations -- such as serial devices connected to terminal servers, or substation to substation communications that are serial, but pass across a broader routable communications infrastructure. Without further guidance, the draft 2 guidance makes it look acceptable for any kind of communications path to be connected to a serial device (such as pilot communications for an electronic protective relay on a bulk electric transmission line). From the draft 2 language, we could conclude that serial device probably would not need to be declared as critical unless it is network connected to the ESP—and even if it was there would be no electronic access requirements to apply. The NOP indicates that today, NERC considers serial devices at the ESP perimeter important enough to enforce a penalty. Draft 2 seems to dismiss the same issue from any regulation. It also seems contradictory that the same section that dismisses serial devices from requirements by virtue of not being routable also requires the inclusion of standalone networks (which are not externally routable) to meet the requirements of an ESP. Must BES Cyber systems that are non-routable reside in an ESP? CIP-007-5 R1.2 requires the disabling of physical input/output ports. Does the disabling of such ports potentially reclassify a device that would otherwise be considered a BES Cyber System? For instance, if a routable device had its physical network ports blocked—what otherwise might be a routable device cannot route. Example: A modern large-screen LCD television is intended to be used for a control center display of real-time operations information. If the TV has “Smart” functions (network application platform), it is more than a peripheral display—it is a programmable computing platform. Such a device used for real-time monitoring meets the criteria for a BES Cyber System. Will physically blocking the network ports reclassify the TV as a simple display peripheral, and allow it not to be subject to all CIP requirements of a BES Cyber System? If such a device is allowed to be neutered into something that would not otherwise be considered a BES Cyber

System, is it no longer subject to other CIP requirements? If so, how would this be distinguished from other device situations—such as a relay control device that directly operates BES transmission equipment, but has no routable connectivity. Is the definition of a BES Cyber System sufficient to provide clarity in more complex situations? Also please see MRO NSRF Comments.
Please see MRO NSRF comments.
No
Yes
Yes
Please see MRO NSRF comments.
No
No
No
No
No
Only some requirements state that they are applicable to “Medium Impact BES Cyber Systems with External Routable Activity”. Since this is the only part of the applicability language that mentions “routable”, it is not clear from the context what the requirement is applicable to. Is the intended meaning a High Impact BES Cyber System is subject to the requirement whether or not it is routable (includes serial devices)? Or is the intended meaning that routable High Impact BES Cyber Systems are all subject to the requirement whether or not it is externally connected (excludes serial devices)? The answer to the above question should clarify whether the CIP-007-5 requirements R1.2, R2.1, 2.2, R2.3, R2.4, R3.3, R4.1, R4.4, R4.5, R5.1, R5.2, R5.4, R5.5, R5.7 apply to non-routable serial devices. With the change to eliminate much of the routable/non-routable language, it is unclear which applicability interpretation to take. CIP-007-5 R1.2 requires the disabling of physical input/output ports. Does the disabling of such ports potentially reclassify a device that would otherwise be considered a BES Cyber System? For instance, if a routable device had its physical network ports blocked—what otherwise might be a routable device cannot route. Example: A modern large-screen LCD television is intended to be used for a control center display of real-time operations information. If the TV has “Smart” functions (network application platform), it is more than a peripheral display—it is a programmable computing platform. Such a device used for real-time monitoring meets the criteria for a BES Cyber System. Will physically blocking the network ports reclassify the TV as a simple display peripheral, and allow it not to be subject to all CIP requirements of a BES Cyber System? If such a device is allowed to be neutered into something that would not otherwise be considered a BES Cyber System, is it no longer subject to other CIP requirements? If so, how would this be distinguished from other device situations—such as a relay control device that directly operates BES transmission equipment, but has no routable connectivity. Is the definition of a BES Cyber System sufficient to provide clarity in more complex situations? Also see MRO NSRF comments.
CIP-007-5 R5.5 states the maximum time between changing any password as 15 months. The Guidelines and Technical Basis section for R5 offers an example password expiration length table that varies based on complexity. It is an interesting table with a good scheme. It also suggests a maximum time length of two years or more for a very complex password. While there seems to be justification for this time period based on the complexity—the table contradicts R5.5’s direct requirements. Is it intended that entities can construct a well reasoned set of password expiration times of any time interval—or is the maximum interval still required to be constrained by 15 months? Also see MRO NSRF comments.
Individual
Jennifer White
Alliant Energy
Yes
No
No
Yes
Yes
Yes

No
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.” [R1] Though we recommend changing “ongoing reinforcement of cyber security practices” to “ongoing reinforcement of security practices” to prevent limiting awareness messages to cyber to the exclusion of physical security awareness, as well. [R2] The main requirement appears to provide programmatic flexibility for the entity to determine which roles to identify. The content identified in Part 2.2-2.10, however, is very specific and may not align with the roles identified by the organization, so there should be some flexibility to omit or make optional some of the sub-requirements for some identified roles. As long as that distinction is programmatically documented, the entity should not fear non-compliance. The way this is it written today, it appears as though all of this training is required for anyone with any type of access. Additionally, some of this training should not be given to someone before the access is granted, based on the sensitivity of the information. Recovery information, for example, should wait until the access is completely authorized and the person has met all prerequisites and other operational training. [Intent?] If the intent of the SDT is that each of 2.2-2.10 should be included in at least one of the roles defined such that all topics are eventually covered by the entity, but not necessarily for every role and not necessarily for “attain” as long as they are covered in “retain” – this is a good intention, but not clearly stated. However, the VSL table is additionally problematic with respect to this intended flexibility. [Proposed Verbiage: R2] Each Responsible Entity shall have a role-based cyber security training program to attain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. The training program(s) must also address elements necessary to retain authorized electronic access or authorized unescorted physical access to BES Cyber Systems. The program(s) must collectively include the assignment of each of the elements in 2.2 – 2.10 to at least one of the identified roles within 2.1. Rationale-the change to “both attain and retain” allows the entity to have programs for attaining that differ from the requirements necessary to retain access, and the existence of two approaches allows the entity to keep sensitive information related to recovery in the “retain” program so sensitive information is not provided prior to access. [Proposed Verbiage: R2.1] Add the following sentence into the main body of the Requirement, immediately following the existing verbiage. “Each identified role must be associated to a minimum of one training content element defined in 2.2 - 2.10 and identified roles must collectively cover content all elements defined in 2.2 - 2.10.” [Recommendation] Remove the reference to the sub-requirements 2.2-2.10 in the VSLs to allow necessary flexibility within programmatic definitions. [Recommendation] If the verbiage recommendation is accepted, the VSLs are fine. If not, the VSLs need to be changed to accurately reflect that each role does not need *every* element. [Proposed Verbiage] for Low, Medium, and High VSLs, add the word “collectively” in front of “include number of the required training content elements….” [R3] Legacy phrasing with regard to the date overall training is required was sufficient as long as it was broad enough to educate those granted physical or electronic access. If corrections are made to R2 to reflect that some of the training elements may be required to “retain” instead of “attain” the following change may not be necessary. Otherwise, more specific, role-based training should be provided within an appropriate timeframe after acquiring certain responsibilities and should be necessary for retaining those responsibilities. The date of the acquisition of those responsibilities should be tied to departmental documentation and roles/responsibilities lists instead of HR reports on official job change. This allows for transitions required by reliable operations, as well as training periods. Also, with respect to demonstrating training when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and what training he or she has received since the very first access was obtained. This could be decades worth of training materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [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. [R4]With respect to demonstrating initial PRA when the access is attained, it forces the entity to maintain a complete history for each person who has ever had access and the PRA he or she had when the very first access was obtained. This could be decades worth of PRA materials, so we’d support the addition of a retention guideline that refers to access attained since the last audit. [Recommendation] Align the measure for R4.4 with the requirement, itself. Change the language in the requirement to include

reference to a vendor contract or legal agreement, and from “verifying” to “assuring.” The measures should be proof of that process or contract rather than what seems to be a copy of the vendor’s actual program. This may be difficult or impossible to achieve. [Proposed Verbiage] Acceptable evidence may include, but is not limited to, the entity’s documented personnel risk assessment program with the criteria, process, or contract identified. These VSLs are fine. [R5] Same intent and assumptions for R4. Additionally, the measures are good. [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.
[R6] This requirement is appropriately written and attainable. Thank you. Recommend changing the VSLs to eliminate zero defect problem. [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. [R7.1]: Recommend changing the verbiage in the last sentence to indicate that the 24 hour clock is related to the initiation, rather than the termination so as not to create two problems should the entity miss the initiation. [Proposed Verbiage] “...and complete the revocation within 24 hours after the effective date and time of the initiation of access revocation." [R7.2]: Too short a time span. Recommend returning to legacy timeframes for job changes within an organization or extending the allowable timeframe based on business days instead of calendar days. For a job change, there is no urgency associated, so weekend access removals are unnecessary. Additionally, there need to be provisions within the Standards for situations where a person will need to straddle two jobs until a replacement is up to speed. [R7.3]: Too short a time span. Recommend extending the allowable timeframe based on business days instead of calendar days. The access removals associated with 7.1 should be sufficient to compensate for the risk introduced by waiting through a weekend for information access removals. [R7.4]: If 'revoke' in this case means to 'delete' the user account from the system, we disagree. [Recommended Verbiage] Change “revoke” to “disable.” [Rationale] We would disable the account and possibly change the account password but when you delete a Windows account you can never reclaim the original GUID that Windows assigns to the unique account. Therefore, reporting, file ownership and anything relating to the GIUD will have been lost and difficult to track past account activity. This may be true for other operating systems as well. [R7.5]: The "out" for extenuating operating circumstances should be applied to all CIP 4 R7 requirements. [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.
No
Yes
Alliant Energy voted “No” on the Standard, as a whole, due to the significance of the changes we propose herein. Agree EEI Comments with respect to moving applicability elements out of the main requirement in the table. Limit applicability to the applicability column. [R1.1] “All BES Cyber Assets…” should apply to BES Cyber Assets associated with High and Medium Impact Sites that have external routable connectivity. There should not be an obligation to create an ESP with an EAP around an otherwise isolated network. This ties into the proposed definition for ESP and should be considered along with that proposed definition. [R1.2] Recommend combining 1.1 and 1.2, after the changes to the applicability and definitions are completed. [R1.4] Recommend changing “where technically feasible” to “within the capabilities of the system.” [R1.5] Change applicability verbiage to Electronic Access Points associated with ESPs at High Impact Sites and Electronic Access Points associated with ESPs at Medium Impact Control Centers. Rationale – the current phrasing would suggest the need to implement external routable connectivity in otherwise isolated networks to meet this requirement. Additionally, the requirement is very subjective and may not be feasible for encrypted communications. This requirement needs to be clarified or stricken. Does this relate to just ingress.

egress, or both? Measures should be written to allow the entity to come up with different, but equally effective solutions. The “and” between the measures implies that both are required, at a minimum. Instead, wholly different options may exist. [VSLs] The percentages are problematic as it is not clear what, exactly, is being measured. How does an entity count or measure External Routable Connectivity? Is it rules, external devices, internal devices, or something else? These need to be written such that they apply to the program, itself, and continues to maintain the zero tolerance approach, and they are not progressive. The Low currently states criteria that aren’t even used in the rest. 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.
[R2] Replace “Where technically feasible” with “Within the capabilities of…” to eliminate the allusion to maintaining the TFE process. Alliant Energy agrees with the EEI comments related to moving the applicability statements out of the requirement and limiting them to just the applicability table. With these minor changes, Alliant Energy supports this requirement and its intentions.
No
Yes
Yes
Alliant Energy was very close to voting “Yes” on this requirement. While most of it is appropriate, the comments mentioned herein warranted a “No” vote until corrected. [R.1] Recommend referring to Electronic Access Control Systems in the same way that Physical Access Control Systems are mentioned for clarity and consistency. The definitions of both take care of the monitoring component, so there is no added benefit to mentioning the Monitoring component again in the language of the Requirement. [R1.1] If we will be measured on implementing, the requirement, itself, should indicate it, rather than just putting that word in the measures. Additionally, the applicability, measures, change description, and main requirement do not align with respect to whether or not EACs or PACs should be protected. There are conflicting messages and they should be corrected. [R1.2] Recommend changing “allow” to “restrict” within the requirement. [R1.4] –The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Additionally, a .1% down time for monitoring security will accumulate for monthly planned outages to implement patches so would like to see allowances for this. A percentage uptime figure should be removed from the standard. Placing specific values such as this should not be included in standards and are a distraction that auditors will try to prove rather than focusing on overall security posture. If an entity can show all outages and maintenance and associated compensating controls during the outage, this is sufficient control, as is required in R3.2 already. Proposed Verbiage: Have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.5]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [R1.6] The identified percentage requires a level of tracking for monitoring that may not be technically feasible. Recommend have controls that monitor the PSP 24X7 with mechanisms for identifying and documenting planned or unplanned outages. [R1.7]: Recommend striking the reference to “within 15 minutes of detection” and, instead, require the documentation of appropriate response timing within incident response plans. [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
No
No
No
No

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.” [R1] – Consider adding a qualifier for external routable protocol on Medium Impact facilities for all CIP-007 R1 sub-requirements to maintain consistency. Refer to the “Change Rationale” provided by the drafting team in R5.6 for the justification for this change. In all applicability columns, (CIP-007) where medium impact facilities are included, recommend including “with external routable connectivity”. [R1.1] Recommend adding the routable connectivity qualifier on the whole of R1, including High and Associated cyber assets. Recommend changing “Where technically feasible” to “Within the capabilities of the system…” Additionally, Alliant Energy supports EEI comments related to the elimination of applicability components within the requirement and move them to the applicability column. Discussion of cyber assets in this context is in direct conflict with the BES Cyber System concept and needs to be stricken. [VSL Recommendation] This VSL is written as a zero tolerance violation. There is also no progression. 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. [R2.1] Alliant Energy agrees with EEI comments related to the inclusion of cyber assets in the requirement, itself, instead of limiting applicability components to the applicability column. Also, the cyber system concept is in direct conflict with a specific requirement applied at the device level. [R2.3] Recommend removing the term “dated” from the action plan to allow waiting for an outage or window that is not yet scheduled. If "dated" cannot be removed, recommend inserting the word "estimated" in front of timeframe. [R2.4] Recommend adding flexibility to change the plan without risking non-compliance. Proposed Verbiage – “For each plan created or revised in 2.3, document the actual implementation date and the reasoning for any discrepancies between the estimated timeframe and actual implementation.” [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. [R3 – R3.3] should be revised to account for the differing methods that can be utilized as part of R3.1. As an example, per R3.1, a company can use policies as a method to deter, detect, or prevent malicious code. If a company were to adopt policies as their method, R3.3 would not be applicable as there would be no malicious code to update. [R3.3] This applicability should be limited to just those systems with External Routable Connectivity. Without that connectivity, the monthly signature updates are not commensurate with the actual risk. Additional verbiage needs to be added to reflect the potential that the only implemented controls are system hardening and/or policies in 3.1. Because these devices tend to be those in TFEs for malware protection, some accommodation must be made here. [R4.1]Proposed Verbiage: “Within the capabilities of the BES Cyber System, log events such that Cyber Security Incidents can be identified and investigated. Event types include: …” [R4.2] Proposed Verbiage: “Within the capabilities of the BES Cyber System, generate alerts for detected security events that the responsible entity…” [R4.3] Recommend striking this requirement or changing the verbiage to “Document the controls implemented to identify and respond to detected logging failures. Document detected logging failures along with any discrepancies between the actual response and the documented response plan.” No reference to a timeframe should be included in the requirement, but it may make sense to require its inclusion in the documented plan. [R4.4] Proposed Verbiage: Remove “Where technically feasible” and precede requirement with “Within the capabilities of the BES Cyber System. [R4.5] Alliant Energy would like clarification on the intent of this requirement. In its current state, it is highly subjective. While we recognize that the possibility exists that system alerts are not working properly and that the entity should be verifying functionality, a manual review of logs in addition to implemented automated parsing and alerting will not add security. The criteria configured into an automated system are intended to match the criteria used by a person manually reviewing logs; it’s just that the automated system allows the immediate and rapid parsing of voluminous records. Alliant Energy would like to understand what security goal is strived for within this requirement. Additionally, this requirement states a “how” without stating a “why,”

which prevents the entity from finding a better or more efficient way of achieving the same goal. Recommend stating the goal within the requirement and leaving it to the entity to define the program that meets the goal. [Proposed Verbiage to add clarity]: “Document and implement a secondary control(s), and an associated interval, not to exceed 2 weeks, to assure the generation, capture, monitoring, and alerting of events as identified in 4.1. Move the summarization or sampling verbiage to the measures. [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.
[R5.1] Propose change to “within the capability and operation of the BES Cyber System” instead of “technically feasible.” [R5.2] The CIP Senior Manager will not have the technical expertise to recognize the actual risk introduced by the presence or quantity of default or generic account types. The turnover rate at the organizational level at which this level of expertise exists would create a prohibitively administratively burdensome process without adding the desired oversight. Recommend striking this requirement or changing to allow designation similar to CIP-004 R6, without direct documentation ties to the Sr Mgr. [R5.4] Recommend changing “technically feasible” language to “within the capabilities of the system or allowable by support vendors.” Proposed Verbiage: “To the extent allowable by the support vendors and capabilities of the system, change publicly-available or industry-known default passwords.” Removed “on cyber assets” to align with the cyber system applicability column. [R5.5] Proposed Verbiage for 5.5.1: “Password length that is, at least, eight characters or the up to the maximum allowable by the system if that maximum is less than eight.” Carry this change through 5.5.2 to add clarity. [R5.6] Don’t touch this one – it’s great as it is. [R5.7] Recommend changing technically feasible language to “Where system capability or operational risk allow, limit the number of unsuccessful…” [VSLs] These are more in alignment with the expectations of the industry. Perhaps a Low and Medium could be created.
Group
ACES Power Marketing
Jason Marshall
No
No
No
No
No
Yes
No
(1) Regarding Question 1 (CIP-004-5 R1): Conceptually, we agree with the requirement and the attempt “to remove the need to ensure everyone with… access ‘received’ ongoing reinforcement” which was expressed in the change rationale for Part 1.1. However, we do not believe the requirement accomplishes this intent. Part 1.1 includes “for the Responsible Entity’s personnel who have authorized… access”. How does a responsible entity prove that it reinforced security awareness to personnel with authorized electronic and/or authorized unescorted physical access unless they maintain a training record for each of these personnel? We think removing “for the Responsible Entity’s personnel who have authorized… access” would help solve this issue. (2) Regarding Question 2 (CIP-004-5 R2): While we agree with the concept that a responsible entity should be able to structure their training to various roles, we believe that Part 2.1 needs to be optional. Smaller entities may find it more cost effective to deliver the same training to everyone rather than develop role based training. As long as it covers all required parts, this should be allowed. (3) Regarding Question 3 (CIP-004-5 R3): Requirement R3 would be clearer if it referenced Requirement R2 rather than repeating much of the language from Requirement R2. Requirement R3 is simply a requirement to implement the training program from Requirement R2. Thus, we suggest replacing everything after “to attain and retain… access” with “required for CIP-004-5 R2”. (4) Regarding Questions 2, 3, 4 and 5 (CIP-004-5 R2, R3, R4 and R5): The main requirements are written such that they apply to all BES Cyber Systems including low impact systems. The risk assessment program is only supposed to cover

the “Applicable BES Cyber Systems and associated Cyber Assets” identified in the Table. After the clause “authorized electronic access or authorized unescorted physical access” within the main requirement, we suggest changing “to BES Cyber Systems” to “Applicable BES Cyber Systems and associated Cyber Assets”. The rationale box for the requirement also needs to be modified. (5) Regarding Question 4 (CIP-004-5 R4): We thank the drafting team for clarifying that the risk assessment is limited to addresses with a duration of six months or more. Short term addresses may not be reported by the employee, vendor or contractor and may not show up in a records check. (6) Regarding Question 5 (CIP-004 R5): The measure for Part 5.2 of Requirement R5 needs to be modified. As written now, the only evidence that it lists is the personnel risk assessment. This is contrary to Part 4.4 of Requirement R4 which describes that the personnel risk assessment program must have a criteria or process to verify that the personnel risk assessment has been performed for vendors or contractors. Having a copy of a personnel risk assessment for non-employees is contrary to some state laws. A simple solution would be to include other types of evidence in the measure such as attestations from contractors and vendors or receipts (or other equivalent forms of evidence) from companies that perform personnel risk assessments that identify the name of the contractor or vendor. (7) Regarding Question 2 (CIP-004-5 R2 VSLs): It is not clear if missing three parts of the requirement is a Moderate or High VSL. Moderate is missing two and High is missing four. (8) Regarding Question 5 (CIP-004-5 R5 VSLs): Given the number of notice of penalties that have been issued regarding personnel risk assessments, it is clear that documentation is difficult to maintain for personnel risk assessments. Thus, escalating to higher VSLs for each missing personnel risk assessment seems excessive and inconsistent with actual penalties that have been issued for missing personnel risk assessments. This is particularly true for employees that have had an annual performance review and are in good standing. For long-tenured employees in good standing, the personnel risk assessment is little more than an administrative check.
(1) Regarding Question 6 (CIP-004-5 R6): For more clarity, we suggest that Parts 6.2, 6.3, and 6.4 should be modified to refer to Parts 6.1.1, 6.1.2, and 6.1.3 respectively rather than just Part 6.1. (2) Regarding Question 7 (CIP-004-5 R7): In Part 7.2, revoking access for employees that have been reassigned or transferred by the end of the next calendar day is too short a time frame particularly for those employees in good standing. (3) Regarding Question 7 (CIP-004-5 R7): Part 7.4 needs to be clarified that revocation of user accounts does not necessarily mean deletion of the accounts. Accounts may need to be disabled due to the unique characteristics of the operating system. Deletion on certain operating systems can have unintended consequences. (4) Regarding Question 7 (CIP-004-5 R7): The measures in Part 7.5 only account for the 30 days within the requirement and not the 10 days after “extenuating operating circumstances”. It needs to account for this latter part of the requirement. (5) Regarding Question 7 (CIP-004-5 R7): There is an extraneous 77 in front of the reference next to the change rationale box. (6) Regarding Question 7 (CIP-004-5 R7 VSLs): The Lower VSL regarding passwords for joint accounts does not make sense. It includes the statement “for one or more individuals”. Since it is a joint account there will always be more than one individual. (7) 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. (8) Regarding Question 6 (CIP-004-5 R6 and R7): Measures for Parts 6.6, 6.7 and 7.1 are inconsistent with the statement in the background section which says that a numbered listed includes all required evidence. The measures specifically say “evidence may include, but is not limited to”. We agree with the actual statement in the measure and believe the background section should be updated. (9) It is not clear why Parts 6.1, 6.4, 6.7 and 7.3 are included in CIP-004-5 R6 and R7 and not CIP-011-1. These parts deal with protecting BES Cyber System Information. Protecting BES Cyber System Information is consistent with the stated purpose of CIP-011-1 but is not consistent with the stated purpose of CIP-004-5. The purpose of CIP-004-5 is essentially to minimize risk from individuals accessing BES Cyber Systems while the purpose of CIP-011-1 is to prevent unauthorized access to BES Cyber System Information. To avoid confusion, we suggest moving them to CIP-011-1.
No
No
(1) In Part 1.1, the requirement and applicability are not consistent. The requirement states that it applies to all BES Cyber Assets which would include low impact BES Cyber Systems. The applicability column limits applicability to high impact and medium impact BES Cyber Systems. For consistency,

we suggest changing “All BES Cyber Assets” to “BES Cyber Assets within applicable BES Cyber Systems” within the main requirement. (2) In the background section, there is no description of “High Impact BES Cyber Systems with External Routable Connectivity” which is included in Part 1.2.
(1) The requirement and definition need to further clarify what constitutes Interactive Remote Access. Is accessing a BES Cyber Asset within the Electronic Security Perimeter from another trusted network (i.e. a company LAN without BES Cyber Systems or BES Cyber Assets) considered Interactive Remote Access or does it only constitute Interactive Remote Access if it is from an untrusted network? (2) Part 2.3 should further clarify multi-factor authentication (MMA). Does MMA apply to the remote session through the ESP, to the Intermediate Device, or both?
No
Yes
Yes
(1) Regarding Applicability Section 4.2.4 Exemptions: This 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-006-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (3) Regarding Question 14 (CIP-006-5 R1): It is unclear how the “operational and procedural controls to restrict physical access” required in R1 Part 1.1 differ from the “physical access controls” required in Parts 1.2 and 1.3. Suggested methods for restricting physical access are given in the “Guidelines and Technical Basis” section, but none are given for “operational and procedural controls.” Additional discussion in the application guidelines on these operational and procedural controls would be helpful in understanding them. (4) Regarding Question 14 (CIP-006-5 R1): The addition of the list (BES Cyber Assets, BES Cyber Systems, etc.) to the main requirement creates ambiguity. This has the effect of including low impact BES Cyber Systems, BES Cyber Assets, etc. into the requirement. In effect, now a documented physical security plan is required for them without any of the requirement parts applying. We suggest either removing the list or adding “applicable” in front of the list to make it clear that only those items in the applicability column are intended. (5) Regarding Question 14 (CIP-006-5 R1): We disagree with including 99.9% availability in Part 1.4 and Part 1.6. First, outages for planned updates will accumulate greater than 0.1% outage time. Second, this refocuses the requirements from enabling requirements that focus on security posture to actual performance. Third, it essentially creates a requirement within a requirement. Fourth, it creates additional unnecessary evidence generation. Not only will the entity have to prove it enabled monitoring but it will have to prove the monitoring worked. If the purpose is to prove monitoring worked, then eliminate the enabling requirements and just state the availability requirement. At least, this way the registered entity only has to show actual availability for evidence. Fifth, availability would be better suited for a responsible entity to use as an internal control for self-assessment of a security program rather than as an enforceable requirement. Sixth and finally, Requirement R3 obviates the need for an availability requirement. R3 compels the entity to maintain and test their physical access control systems and to document any outages. Thus, availability is likely to be as high as reasonably possible which may not quite reach 99.9%. (6) Regarding CIP-006-5 R1 and R2: Parts 1.9 and 2.3 regarding data retention belongs in the evidence retention section. Otherwise, it is in direct conflict with the statement “shall retain data or evidence for each requirement in this standard for three calendar years” from the evidence retention section. (7) Regarding the VRF for CIP-006-5 R2: A visitor control program is intended to identify and log visitors to the Physical Security Perimeter (PSP). They cannot gain access due to other requirements such as CIP-006-5 Requirement R1 that compels the responsible entity to establish physical access controls. Furthermore, the training requirements of CIP-004-5 compel a responsible entity’s personnel with authorized unescorted physical access to have been trained on who has access and that visitors must be escorted. Thus, the visitor control program can only be an administrative function that is truly intended to keep track of those visitors that have been to the PSP. By definition, administrative requirements should have a Lower VRF. Thus, CIP-006-5 Requirement R2 should have a Lower VRF. (8) Regarding CIP-006-5 R2 VSLs: A Lower VSL could be written. For example, missing one entry in the in the visitor log could be written as a Lower VSL rather than a Moderate VSL. (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.
Yes
Yes
Yes
Yes
Yes
(1) Regarding Applicability Section 4.2.4 Exemptions: This 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-007-5 or the section 4.2.4 should be struck if it truly only applies to CIP-002-5. (2) Regarding the Applicability Section please see comments submitted by ACES Power Marketing regarding Applicability in Comment Form A, Question 3, Comments 6-9. (3) Regarding the VSLs for CIP-007-5 R1 - Because there are likely many ports for Requirement R1, the four VSLs could be written based on the percentage of ports missing from documentation. (4) Regarding the VSLs for CIP-007-5 R2-4 - For Requirements R2-R4, there will likely be many BES Cyber Systems to which the requirements apply. Four VSLs could easily be written based on the number of BES Cyber Systems for which the requirement was missed. (5) Regarding CIP-007-5 R4: Part 4.4 regarding data retention belongs in the evidence retention section. Otherwise, it is in direct conflict with the statement “shall retain data or evidence for each requirement in this standard for three calendar years” from the evidence retention section.
Individual
David R. Rivera
New York Power Authority
No
No
Yes
No
Yes
Yes
No
NYPA agrees with NPCC comments, plus - In R2 Part 2.10, “training content on risks associated” – it’s not clear what is required. Awareness and other training (i.e. part 2.4) would cover this area in general; we don’t believe that this specific training module is required.
NYPA agrees with NPCC comments.
No
No
NYPA agrees with NPCC comments, plus – In R2, allow an exclusion for the devices that accessed or interrogated in a read-only mode.
NYPA agrees with NPCC comments, plus – In R2, allow an exclusion for the devices that accessed or interrogated in a read-only mode.
Yes
Yes
No
In R1 (parts 1.4 and 1.6), the references to 99.9% availability are not clear. There is no guidance as to how this can be measured; therefore recommend removing the availability reference as the entity will already have compensating measures in their physical security plan. Also, how is one to know unauthorized circumvention?
Yes
No
No
No

No
NYPA agrees with NPCC comments.
NYPA agrees with NPCC comments, plus – In R5.1, is too restrictive and expansive for 'Medium' BES Cyber Systems. We suggest replacing "all user access" with "access to configuration or programming resources" or "cyber access".
Individual
Tracy Richardson
Springfield Utility Board
No
Yes
Yes
Yes
Yes
Yes
No
SUB agrees with CIP-004-5 Requirements R1, R2, R3, R4, and R5 not being applicable to Low Impact BES Cyber Assets and BES Cyber Systems.
In Part 7.2 Requirements for reassignments or transfers, "by the end of the next calendar day" does not take into consideration weekend days. SUB would recommend "by the end of the next business day" for High and Medium Impact. SUB agrees with CIP-004-5 R7 not being applicable to Low Impact BES Cyber Assets and Cyber Systems.
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Robert Mathews
Pacific Gas and Electric Company
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes

Yes
No
Yes
Yes
R1.4 is unacceptable as stated. Rationale: While the recognition that 100% availability of the monitoring systems may not be feasible is good, the specific requirement for 99.9% availability has no technical basis and likely will result in imprudent use of resources to provide the specific data needed to demonstrate performance to this specific level for a large quantity of devices or processes, many which may not have the capabilities to even provide the data necessary to perform an availability calculation. In the Guidelines and Technical Basis section for R1 on page 28, Alarm Systems and Human Observation are mentioned as methods to monitor physical access. Measuring the availability of human observation or components of an alarm system such as door or window contacts to the 99.9% threshold is likely not feasible or prudent. Suggest Standard Revisions: Have controls that monitor the Physical Security Perimeter for unauthorized circumvention of a physical access control into a Physical Security Perimeter.
Yes
No
No
No
Yes
Rationale: Medium Impact BES Cyber System without External Routable Connectivity (isolated computer systems) should not be subject to the same requirements in R2.1, 2,2, 2.3, 2.4; R3.1, 3.2, 3.3 and R4.1 as those with external routable connectivity. For example some systems without external routable connectivity cannot employ monitoring, patching and malicious code protection mechanisms used on systems with external routable connectivity. Suggest Standard Revisions: Revise R2.1, 2,2, 2.3, 2.4; R3.1, 3.2, 3.3 and R4.1 applicability to Medium Impact BES Cyber Systems with External Routable Connectivity
Group
SPP and Member companies
Lesley Bingham
Yes
No
Yes
Yes
Yes
Yes
No
CIP-004-5 R2.2-2.10 contain elements which can comprise a training program. If role-based training is required (as indicated by R. 2.1), can a Responsible Entity choose from those elements to create a training program for different roles? Or must all roles identified receive some training from each of the elements in R. 2.2-2.10? If all roles must receive some training for each of the elements in R. 2.2-2.10, what is the value of having role-based training? If all roles must receive some kind of training on all elements of R. 2.2-2.10, we would recommend adding the following language to each of the sub-requirements: Training content should be provided to each identified role based on the level of understanding needed for each. Each identified role must [or must not if Responsible Entities can choose which elements to include] be provided training on this element.
Table 7 is focused on Access Revocation and the time guidelines called for are stringent. While no one advocates orphaned accounts, the HR and IT processes which must support access revocation can take time and cause conflict with these standards, at best or non-compliance, at worst. The processes are designed to capture appropriate approvals, create a trail of activity which can be used as audit

evidence, and other activities which are designed to provide compliance. Realistically, these efforts take time—time which the standard does not allow for. Smaller entities without an on-call staff will have difficulty complying. Terminations are not uniform and may call for different responses. The 24 hour timeframe does not allow for consideration of a response which may be appropriate for the situation. The language in 7.5 acknowledging extenuating circumstances would be a helpful addition to Part 7.1, 7.2, and 7.3 The Measures in 7.1 suggest that a system-generated workflow is required. Managing the trail of activities for a termination can easily be managed via emails sent from activity initiator to approvers, on to implementation resources and an email back to the group when the access is revoked. Is such a “paper trail” considered adequate? The Measures in 7.2 do not provide additional security and extend what is already a time-sensitive and time consuming process. Also recommend changing these to a list of bullets from numbers and removing the “and” from the first item. Part 7.3 should be accomplished as required when Part 7.1 is completed. To have a separate item for this seems to be little more than an audit trap. The Measure for 7.5 does not indicate what would be appropriate evidence for the “extenuating operating circumstances”. If documentation is required, the measure should state “Additional documentation for ‘extenuating operating circumstances’ consists of an overview of the situation, approval by the CIP Senior Manager or delegate, and attestation that the situation has been addressed” or other concrete examples.
No
Yes
1. Part 1.3 requires monitoring and documentation of all outbound traffic. While such is absolutely a good practice, it will be an expensive burden for many entities. If monitoring only inbound traffic for a Physical Security Perimeter is deemed to be adequate, it should be adequate for the Electronic Security Perimeter. Recommend dropping requirement for outbound traffic. 2. Part 1.4 assumes that there will be dial-up connectivity in the ESP of all Responsible Entities. How can an entity prove a negative if they do not allow dial-up? Recommend adding a sentence to the requirement which states “Dial-up connectivity may not allowed by all Responsible Entities and this requirement may not apply for all situations.” Recommend adding a sentence to the Measure to state “Evidence may include an attestation of connectivity options where dial-up connectivity is not present in a Responsible Entity’s ESP.” 3. The Measures in Part 1.5 are still heavily centered on a single technology as the primary means of compliance—Intrusion Detection Systems. Recommend adding language to lessen focus on IDS. Examples could include “Evidence that intrusion detection or other monitoring systems are functioning” or “Documentation showing where intrusion detection or other monitoring systems are deployed.” It’s also important to note that “malicious” activity cannot be determined strictly by watching for an activity. Traffic to an ESP which is malicious may in fact appear to be normal. The qualification of “malicious” vs “normal” requires knowing an actor’s intent, which cannot always be gleaned from log entries.
No
Yes
Yes
1. Part 1.4 requires a specific availability requirement that may be hard to measure for some controls. For example, how do you measure the availability of a guard? While availability targets are certainly valuable, defining this narrowly will provide a burden for tracking and measuring for entities. 2. Part 1.6 requires a specific availability requirement that may be hard to measure for some controls. For example, how do you measure the availability of a guard? While availability targets are certainly valuable, defining this narrowly will provide a burden for tracking and measuring for entities. 3. Part 3.2 requires documentation of outages for the physical access control, logging and alerting systems. This would be a better place for the availability requirements currently in Part 1.4 and 1.6.
Yes
Yes
No
No
Yes
1. Part 1.2 and Part 2.1 have better language than the previous release of the standard. Specifically, it is helpful that the Standard Drafting Team recognizes that some devices are not able to be updated.

2. Part 3.3 is confusing. Breaking this up into separate sentences will provide clarity. Recommend “Update malicious code protections that use signatures or patterns at least once within 35 calendar days of each available signature or pattern release. This does not require use of every available release, but where a release is available, at least one update has occurred within 35 calendar days from that release. If a Responsible Entity determines and documents that specific updates of signature or pattern releases will negatively affect the Cyber Asset or BES Cyber System, those specific releases are not required to be applied.” 3. Part 4.1 needs to include the “capable of detecting” in the Requirement and not solely in the measure. Recommend “Log events, where the System is capable of detecting such, for the identification of….” Part 4.1.4 requires the logging of “malicious activity”, but analysis of intent is required to determine if an action is malicious. The disagreement here is not to say that the industry shouldn’t do logging of sufficient information for adequate Cyber Incident Response. What should be avoided is language which could allow an auditor to request a list of all log data which shows malicious activity. Any log file will only record what actions were taken—not the intent behind the actions. Recommend language “log user and system activities determined to be indicators of misconduct”. Part 4.2 again uses the phrase “malicious activity” and the same objections apply. Recommend use of “suspicious”, “unusual” or “detected activity which the Responsible entity determines as not normal”. Part 4.5 requires a manual review of logs for which the Responsible Entity has already generated alerts. Recommend changing to “Review a summarization or sampling of logged events that the Responsible Entity has determined could identify previously undetected Cyber Security Incidents. Such a review will be conducted every two weeks at a minimum.”
1. Part 5.1 only mentions user accounts and does not address the other types of accounts covered in the table in the Application Guidelines. If user account is a distinct term separate from the other types of accounts in the table, then User Account should be defined in the Definitions and should clarify that the term addresses interactive accounts used by individual persons. This would be distinct from system-to-system process communications. Such accounts should have initial and annual password change requirements and robust password composition requirements. System accounts should also be defined to clarify that these are non-interactive accounts which may be installed on a device from the manufacturer or required for use software, but will never be used during a login process by an individual person user. These accounts can have other protections, but should not be subject to the initial password change or annual password change requirement. These accounts are not generally built in a way which allows for uncomplicated password changes and such changes can be highly disruptive to the devices where they exist. Often, touching these accounts for a password change puts the reliability of the device at a higher risk than the risk of a long-used password. The table in the Application Guidelines is helpful, but since it is not a part of the standard, Responsible Entities will not be able to take advantage of the assistance of the types of accounts noted and the suggested periodicity of password change. Adding this table to the plain language of the standard could be beneficial to Responsible Entities. 2. Part 5.5 is an improvement in password composition language. Thank you for your efforts, Standard Drafting Team. 3. Part 5.6 could be clarified to be applied to only individual user accounts with the addition of this sentence at the end of the requirement: “This is not intended to apply to non-interactive, non-user assigned accounts.”
Group
IRC Standards Review Committee
Christine Hasha
Yes
No
No
No
No
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 8. The IRC respectfully provides these additional comments. The IRC requests that CIP-004-5 Measure 1.1 (question 1) be changed from “but not limited to” to “but is not limited to”. This is consistent with the other measures contained within the standard.

The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 9. The IRC respectfully provides these additional comments.
Yes
Yes
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 12.
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 13.
No
Yes
No
The IRC supports the comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) regarding question 17. The IRC requests that CIP-006 Requirement 1.4 and 1.6 (question 14) be modified from “Have controls” to “Have control(s)”. The IRC requests that CIP-006-5 Requirement 1.5 and 1.7 (question 14) remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not cyber. Request that Requirement 1.5 be revised to “Issue an alarm or alert in response to detected unauthorized circumvention of a physical access control into a Physical Security Perimeter within 15 minutes of detection.” Request that Requirement 1.7 to “Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System within 15 minutes of the unauthorized physical access.” The IRC requests that CIP-006 Measure 2.2 (question 15) be modified to “Evidence may include, but is not limited to, records of manual or automated logging of the entry and exit of visitors into the Physical Security Perimeter that includes date and time of the initial entry and last exit, the visitor’s name, and the name of an individual point of contact responsible for the visitor.”
Yes
Yes
Yes
No
Yes
The IRC supports comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) on the following items. • The 30-day timeframe in CIP-007-5 R2.2 should be increased to at least 35 days to allow for monthly processes. • The applicability of CIP-007-5 R2.1, R2.2, R2.3 and R2.4 to “Medium Impact BES Cyber Systems” should be limited to “Medium Impact BES Cyber Systems with External Routable Connectivity.” The exclusion of cyber systems/assets with no routable connectivity will eliminate a significant burden of tracking and documentation requirements associated with serially connected devices that would have minimal impact to reliability. This is particularly burdensome for systems that are geographically dispersed and would require direct personnel interaction and physical access to each device to deploy patches to non-externally routable systems. • Under measures, M2.4 bullet 2 should be revised to read “Records of implementation of vendor recommended or other appropriate mitigations;” to eliminate any misunderstanding and allow for appropriate mitigation plans that are different than a vendor-recommended plan. • Modify Requirement R 4.1.3 from “detected and logged malicious software…” to ”detected and logged malicious code…” • Eliminate requirement R4.1.4. The term “malicious activity” is ambiguous. • Modify Requirement 4.2.1 to read “detected events per R4.1; and” The IRC requests that CIP-007-5 Requirement 3.1 (question 20) be modified to remove strike the word “deter”. Deter and prevent are redundant of each other. The IRC requests that CIP-007-5 Requirement 3.3 (question 20) be modified as, “For signature- or pattern-based malicious code protections, update the signatures or patterns within 35 calendar days of each available signature or pattern release. Signature or pattern releases may be grouped together for the 35 day update. This excludes releases that negatively affect the Cyber Asset or BES Cyber System.” The IRC requests that CIP-007-5 Requirement R4.1 (question 21) be modified as, “Log events for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events, where technically feasible:” The IRC requests that CIP-007-5 Requirement 4.5 (question 21) be modified as, “Where manual logging is used, review a summarization or sampling of logged events at a minimum every two weeks to identify undetected Cyber Security Incidents.” This should only apply where automated processes and alerting are not

possible.
The IRC supports comments filed by the Texas RE NERC Standards Review Subcommittee (NSRS) on the following items. • In Requirement R5.1, authentication should be done for accounts, not for user access. Suggest revising to read “Enforce authentication of accounts when accessing applicable Cyber Assets, where technically feasible”. • CIP-007-5 Part 5.4: Recommended change, “Change known default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” This allows for unique passwords. • CIP-007-5 Part 5.7: Recommended change, “Limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts, where technically feasible.” Please provide guidance on what is considered a suitable minimum threshold. The IRC requests that CIP-007-5 Requirements 5.2 and 5.3 (question 22) have the same applicability. Requirement 5.3 should be modified to remove “with external routable connectivity” from the applicability. The IRC requests that CIP-007-5 Requirement 5.2 (question 22) be modified to “delegate(s).” The IRC requests that CIP-007-5 Measure 5.3 (question 22) be modified to, “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” The IRC requests that CIP-007-5 Measure 5.5 (question 22) be modified to, 5.5.1. Password length that is the lesser of: • At least eight characters; or • Maximum length supported by the Cyber Asset; and 5.5.2. Password complexity that is the lesser of: • Three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric); or • Maximum complexity supported by the Cyber Asset. The IRC requests that CIP-007-5 Measure 5.5 and 5.6 (question 22) be modified to remove reference to attestations. Some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states “Documentation of the registered entity’s procedural solution and training program to educate its affected personnel on its procedural solution.”
Individual
Gregory Campoli
NYISO
Yes
Yes
Yes
No
Yes
No
No
• Please clarify R4 4.2 for how six months is applied • Please clarify how R6.5 requires quarterly review for authorization with R6.6 and R6.7 annual really includes a complete review. Don’t the same “shared” accounts count in both R6.5 and R6.6?
• R7.4 should refer to R7 part 7.1 and 7.3 • R7 Measure change “removal” to “revoke” to be consistent with requirement. • R7 VLFs should be consistent
No
No
• Recommend removing “but is not limited to” from R1 1.1. • R1.5 change from “intrusion detection” system to “detection system”. • Measure 1.7 IDS is too prescriptive and recommend more generic language.
• There appears to be technical conflict in R2.2 between using encryption and IDS monitoring as SSH would prevent IDS from identifying events depending upon implementations. • R2.3 should reference “Multi-factor” solution but not be limited to list as some place you are or other options may be a solution.
No
No
Yes
• R1.3 don’t start with TFE and refer to multifactor control • R1.4 remove 99.9 availability to allow for alternative physical controls with guards as mitigation. • R1.5 a security guard could perform the detection, alerting and response so they would document the event… • Parts 1.5 and 1.7 remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not

cyber. • Part 1.5 Revert to the wording that was in the previous draft of CIP Version 5. • R1.6 remove 99.9 availability to allow for alternative physical controls with guards as mitigation. • CIP-006 R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement.
No
No
Yes
No
No
• R5 – Can multifactor replace passwords without a TFE?
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Yes
Yes
Yes
Yes
Yes
No
No
: 6.1: It is not clear of the individual(s) must be identified by name or if it can be by title. FEUS requests the SDT clarify. 6.1.3: 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. 6.4 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 6.1.3 – 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. 6.7: See comments for 6.1.3 and 6.4 7.3: FEUS feels this would be better defined by an entities Information Protection Program; see comments in R6 regarding the physical location of System Information
Yes
Yes
Yes
Yes
Yes
R1.4 and R1.6 the SDT should define what periodicity the 99.9% availability is determined (monthly, quarterly, annually)
Yes
Yes
Yes
Yes

Yes
Individual
Maggy Powell
Exelon Corporation and its affiliates
No
No
No
No
No
Yes
No
CIP-004-5, R1: We appreciate that the standard consolidates the descriptions of Applicable BES Cyber Systems and Associated Cyber Assets into section 5 to make the table column headings more readable. To clearly direct readers, a notation added to the column heading referencing where to find the descriptions would be useful. CIP-004-5, M1: M1.1 - the list of evidence of distribution options should read "or" rather than "and". The guideline language reinforces that evidence of distribution does not require many or all of these items to demonstrate compliance. CIP-004-5, R2: Further clarification is needed to avoid requiring that every person with access receive training on each topic in 2.2 through 2.10. Training programs should have the latitude to define the type and depth of training appropriate to the role the person has. If all are to train on every topic at depth, it contradicts the concept of role-based training and creates an extraordinarily cumbersome training program. Consider the following revision to R2.1: "Identification of each role and applicable training as defined in R2.2 through R2.10 required for each role." CIP-004-5, R2, R3, R4: The use of the terms "attain" and "retain" are awkward. Consider replacing "attain" and "retain" with "acquire" and "maintain" respectively in R2, R3 and R4. CIP-004-5, R5/M5: We appreciate the acceptance of attestations from contractors or service vendors verifying PRAs.
CIP-004-5, R7: The timing requirements dictated in the requirements indirectly require that entities automate their access programs. As a consequence, automation creates added complications in managing access revocation, for instance, defining what distinguishes a transfer. A new office location or phone number may or may not be a transfer. Further, it's not clear why access revocation requirements for transfers are more stringent than for terminations. The added 30 days for terminations would be valuable for transfers as well. Further latitude within the requirement language is needed to allow internal management of transfers.
No
Yes
CIP-005-5, R1: We recognize and appreciate that the qualifier "technically feasible" gives entities the needed flexibility to meet the security goal in circumstance where the stated requirement is not feasible. It may be useful to clarify in the background or guideline that if not technically feasible, entities are expected to go through the TFE process. Further, NERC Staff should recognize that the Rules of Procedure will likely need revision to accommodate the revised standards that allow for technical feasibility exceptions. The request to approve the ROP revisions should be submitted concurrently with the filing of CIP V5. CIP-005-5, Page #s: One minor note, the page numbers on pages 10-15 of CIP-005-5 are not showing as the others do.
No
No
Yes
CIP-006-5, R1: 1.4 and 1.6 includes a 99.9% availability. We appreciate the latitude to allow for some outage without creating a compliance burden, but greater clarity is needed on how the 99.9% is measured. How was this percent chosen? What goes into the calculation? Does maintenance count? What period is covered to measure? etc. As well, this proposal prompts demonstration of compliance

questions such as what period of time should records cover to demonstrate compliance, etc. CIP-006-5, R1 VSL: We understand the logical basis for the different treatment of dial-up, and previous discussions of CIP-006 and treatment of dial-up is clear; however, the Severe VSL under R1 specifically calls out dial-up. Please clarify expectations concerning BES Cyber Systems with dial-up connectivity either by removing the reference in the VSL or further discussion in the guidelines. CIP-006-5, R2: The wording in 2.2 is awkward: "Require manual or automatic logging of the entry and exit of visitors into the Physical Security Perimeter …" One cannot exit into something. Consider the revision: "Require manual or automatic logging of visitors for entry to and exit from the Physical Security Perimeter …"
No
No
Yes
Yes
Yes
CIP-007-5, R1: M1.1, bullet two should allow for listings of classes of Cyber Assets as in bullet one. Consider revising the second bullet in M1.1 to read: "Listings of the listening ports on the Cyber Assets or class of Cyber Assets from…" CIP-007-5, R2: R2.3 needs revision to clarify the timing expectations. Thirty days from the evaluation completion is acceptable to create a plan; however, revising the plan should be allowed as information and circumstance dictates. The timing should not impose restrictions on prudent revisions to plans. For instance, information regarding a patch may be discovered while testing in the environment indicating that the patch may be harmful or may fail in the environment. A revision to the plan should be allowed to accommodate such new information. Further, the patch implementation should not be required merely to meet a compliance obligation when risks to implementation are discovered during testing or other information sources. The requirement language may need additional language to allow for patch failure. CIP-007-5, R2.4 and R3.3: please offer guidance on what/how much information is expected to demonstrate implementation of a patch plan and implementation of updated signature or pattern files every 35 calendar days. A representative or statistical sample should be acceptable for compliance.
CIP-007-5, R5: The SDT should better align the guidance language to match the requirement language.
Individual
Scott Kinney
Avista Corp
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
See comments provided by EEI
See comments provided by EEI
Group
CenterPoint Energy
John Brockhan
Yes
No
No
No
Yes
Yes
Yes
R2 - CenterPoint Energy believes that the current wording for the training standards creates unnecessary complexity for training, especially entities that may have designed one, all-

encompassing program for compliance with the current version of the CIP Standards. CenterPoint Energy also requests clarification for this requirement and sub-requirements for whether each trainee has to receive all training specified in 2.2 - 2.10. or could the program for each trainee be selective as some information should not go beyond system administrators to protect systems security. CenterPoint Energy recommends the following wording: ""Each Responsible Entity shall have a cyber security training program appropriate to job function…" . R3/R4 – CenterPoint Energy requests clarification on which Associated Physical Access Control Systems/Associated Electronic Access Control or Monitoring Systems are in scope. The Company proposes that the requirement applies to those systems associated with High Impact and Medium with External Routable Connectivity only. R3.2 – CenterPoint Energy proposes that the Standard Drafting Team consider combining 3.2 with 3.1. R4.2 – Under Measures, CenterPoint Energy recommends the wording "As described in Requirement 4.2" instead of "in accordance with this part."
R6 - CenterPoint Energy requests clarification on the term "stored". Is this term used to refer to electronic copies? R7.1 and R7.2 – Under Measures, CenterPoint Energy recommends changing the numbered list to bullets and replacing "and" with "or". R7.2 - CenterPoint Energy agrees with the comments submitted by EEI and NSRS that access for reassigned or transferred employees should not require revocation by the end of the next calendar day.
No
No
R1.1 - CenterPoint Energy recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability as the Company believes that if there is no external connection, the risk is low. If a bad actor penetrates the Physical Security Perimeter, then the device login passwords are defense from unauthorized user access. R1.3 – CenterPoint Energy also recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for this requirement as the application of this control to a non-networked environment does not appear logical. R1.5 – It appears that the measures are focused on intrusion detection systems. CenterPoint Energy proposes that the SDT add "or other monitoring systems" after intrusion detection systems.
R2.1/2.2/2.3 - CenterPoint Energy also recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for this requirement as the requirements reference external remote access. CenterPoint Energy also agrees with the comments submitted by NSRS.
No
Yes
No
R1.1- CenterPoint Energy prefers the Draft 1 version of the measures for this requirement. ("Evidence may include, but is not limited to, documented operational or procedural controls exist and have been implemented.") R1.4 – CenterPoint Energy strongly disagrees with the 99.9% availability statistic introduced in this draft. CenterPoint Energy suggests that the SDT consider provisions for exceptions or manual monitoring and revise the percentage referenced. R1.5 – CenterPoint Energy requests clarification on the term "detected". R1.6 - CenterPoint Energy recommends that the measures be revised to read "access to the "Physical Access Control System". Additionally, CenterPoint proposes that the SDT combine 1.4, 1.5, 1.6, and 1.7. R1.8 – CenterPoint Energy has strong concerns regarding the manageability of this requirement. Attempting to apply this requirement to facilities in the field (i.e. substations) is onerous and adds little to actual security. The Company is concerned that some entities may need to make extensive and expensive changes to some of their facilities to comply. In addition, the Guidelines and Technical Basis states that FERC Order 706, paragraph 572 does not require two or more different and complementary physical access controls; therefore, CenterPoint Energy recommends deleting the requirement. If the SDT is determined to leave the requirement, CenterPoint Energy recommends deleting the Medium Impact applicability. Even with this reduced applicability, CenterPoint Energy recommends adding to the Measures "Video recording; Electronic capture of video images of sufficient quality to determine identity". CenterPoint Energy also generally agrees with the comments submitted by EEI and NSRS.
No
No
No
No

No
R1.1 - CenterPoint Energy requests that the SDT clarify "needed" and recommends replacing the term, “listening”, with enabled. R1.2 – CenterPoint Energy recommends that the SDT remove "signage" from the measures. The Physical Security Perimeter and logical disabling where possible should be sufficient to reasonably protect against unauthorized use. R2.1 – 2.4 – CenterPoint Energy agrees with the comments submitted by EEI in the proposal to add “with External Routable Connectivity” to the Medium Impact applicability. R3 - CenterPoint Energy proposes that the SDT add “with External Routable Connectivity” to the Medium Impact applicability as the requirement cannot be implemented in absence of remote access. R4.1 - CenterPoint Energy proposes that the SDT add “with External Routable Connectivity” to the Medium Impact applicability. CenterPoint Energy recommends adding “where the BES Cyber System is capable” after “Log events” since some legacy systems may not be capable of logging all the events specified in R4.1.1 – R2.1.4. CenterPoint Energy also recommends removing R4.1.4 because the term “malicious activity” is ambiguous and requires an analysis of intent. R4.3 – CenterPoint Energy recommends that the SDT add “after discovery” to the requirement.
R5.2 – CenterPoint Energy agrees with the comments submitted by EEI and recommends deleting this requirement. The requirement may be a problem during storm restoration or emergencies and ultimately, effect reliability. R5.5 – CenterPoint Energy recommends that the measure related to an attestation be deleted as it is not apparent what an attestation will provide that the policy/procedure will not. R5.6 – CenterPoint Energy recommends that the measure related to an attestation for this requirement be deleted and replaced with procedural documentation. CenterPoint Energy also generally agrees with the comments submitted by EEI and NSRS.
Individual
James Tucker
Deseret Power
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
No
No
Yes
R1.4 – The requirement for 99.9% availability for physical security perimeter controls is problematic due to requiring tracking of availability without defining a time period for determining the percentage. The SDT needs to revisit this requirement to reduce the complexity of tracking such availability and to create a clear requirement on this issue.
Yes
Yes
Yes
Yes
Yes

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.
Group
Tri-State G&T - Transmission
Tracy Sliman
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
Steve Alexanderson
Central Lincoln
Yes
Yes

Yes
Yes
Yes
Yes
Yes
Thank you for removing low impact.
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. 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
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. 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.
We’d still like to know where to find the “Secure Remote Access Reference Document” referenced in the Guidelines section under R2.
Yes
Yes
Yes
1. Thank you for removing low impact. 2. 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
Yes
Yes
This does not relate to any of the requirements, but since no question was provided for Applicability, we are putting our comment here. 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.
Thank you for removing low impact.
Group
PacifiCorp
Sandra Shaffer
PacifiCorp support comments submitted by EEI.

Individual
Russell A. Noble
Cowlitz County PUD
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Yes
Individual
John Tolo
Tucson Electirc Power
Yes
Yes
Yes
Yes
Yes
Yes
No
General comment: Agree with EEI's comments to insert "unescorted" into "authorized electronic" references. This allows the access needed for vendor support which was deemed not in the language of the standard in interpretation of CIP-004 for WECC
R7 – TEPC feels the timing should be based on the determination of when access is not necessary, rather than the date of the transfer. The SDT seemed to recognize that the reassignment date might not align with when access was no longer needed, and that a determination was needed. However they did not carry that through to the date of revocation. Suggested wording: For reassignments or transfers, revoke the individual's electronic and physical access that the Responsible Entity determines is not necessary by the end of the next calendar day following the determination. TEPC also agrees with EEI's statement for R6.2: The individual(s) designated in Part 6.1 shall authorize unescorted physical access that the Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances." To "The individual(s) designated in Part 6.1 shall authorize unescorted physical access into Physical Security Perimeter(s) that the

Responsible Entity determines is necessary for performing assigned work functions, except for CIP Exceptional Circumstances.", in order to scope this requirement to the PSP.
Yes
No
R1.4 TEPC agrees with EEI's comment: This requirement is very similar to CIP-007-5 R5.1, with the exception of dial-up applicability. Propose adding BES Cyber Assets with dial-up connectivity used within High and Medium Impact facilities into CIP-007 R5.1, and removing R1.4 from CIP-005-5. This identifies all BES Cyber Assets that require authentication into a single requirement, resulting in a more concise standard. CIP-007 R5.1 already seems to require this, without the specific wording. This could result in double jeopardy.
Yes
Yes
Yes
Yes
No
Yes
No
No
TEPC agrees with the following EEI comments: for all sub-requirements limit scope to Medium Impact BES Cyber Systems with External Routable Connectivity instead of just Medium Impact. Without this change, the patching will apply to closed networks, greatly increasing resource requirements; and R2.2, change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency. TEPC feels for R4.1 that the TFE should be related to the logging, which takes place at the system level, rather than in 4.2 for the alerting; R4.2 – Remove the TFE from this requirement. TEPC also agrees with the EEI comments for R4.
TEPC agrees with EEI comments for R5. R5.1, R5.4: Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routability or dial -up". Rationale: Consistency with CIP-004 R6.2; R5.2: Delete requirement since it's covered by CIP-004 R6.2; and R5.3: Delete requirement and move rationale to CIP-004 R5 since it's covered by CIP-004 R6;
Individual
Oscar Alvarez
Los Angeles Department of Water and Power
Yes
Yes
Yes
Yes
Yes
Yes
No
LADWP does not have extensive comments on this matter at this time.
The proposed time limits for revoking access upon terminations and transfers for the next calendar day present extreme challenges, especially when taking into consideration terminations or transfers that occur on Fridays. More time needs to be given. The next business day for terminations and 3 business days for transfers will make these processes manageable.
Yes
Yes
LADWP does not have extensive comments on this matter at this time.
LADWP does not have extensive comments on this matter at this time.
No

No
No
R1.1 defines operational or procedural controls to restrict physical access to Associated Systems. Need to remove applicability of this requirement for Associated Systems. Existing Standard Operating Procedures address and restrict physical access to Associated Systems. Demonstration of existing procedures should be sufficient to meet the intent of this requirement. R1.3 requires utilization of two or more different and complementary physical access controls. This presents technical challenges and may not create additional security. One control should suffice. Depth of defense already exists through gates, security personnel and card reader systems. The current requirement of one or more physical access methods has been implemented with little or no problems encountered. The increase to two or more physical access controls may bring about unintended consequences and complexity. NERC should provide compliance feedback to industry demonstrating that "one or more" physical access methods have proven ineffective. Additionally, High Impact Control Centers typically have stringent physical security controls and monitoring. R1.6 does not address access log retention. The preference is to maintain a log retention timeframe of ninety calendar days. A log retention timeframe of ninety days maintains the status quo. R3 requires maintenance and testing every 24 months. We prefer that the maintenance and testing cycle be no longer than three years. Equipment failure rates do not support the need for maintenance and testing every two years. Manufacturer mean time before failure rates are in excess of three years. We believe maintaining the three year cycle is reasonable and effective. Additionally, equipment is monitored and malfunctions are reported immediately, thus negating the need for a two year maintenance and testing cycle.
Yes
Yes
Yes
No
Yes
R4.3 requires that before the end of the next calendar day to activate a response to detected event logging failures. This presents a very short time frame to come up with a way to rectify an issue that may require extended investigation. Entities require more time to research and investigate logging failures to come up with a recommended response.
LADWP does not have extensive comments on this matter at this time.
Individual
Tony Kroskey
Brazos Electric Power Cooperative
No
No
No
No
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.
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
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.
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
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
Yes
Yes
Yes
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.
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
Yes
Yes
Yes
No
In Requirement R1.1 in the phrase "…ongoing reinforcement of cyber security practices," the term "cyber" often is understood to mean computer or electronic. PSE recommends dropping the word "cyber" from the phrase in order to make clear that the requirement for a security awareness program would address both cyber and physical awareness topics. In the Measure for R1.1, the evidence required includes the "documented security awareness program." PSE feels that evidence of the distribution and materials associated with the quarterly reinforcement, and the audience of that material should be sufficient and that a documented awareness program is beyond what would be necessary to show compliance with the requirement. PSE recommends removing the requirement for the documented awareness program from the measures as required evidence. PSE views the granting of authorized electronic or authorized unescorted physical access as being dependent upon 1) the successful completion of a personnel risk assessment (PRA), 2) successful completion of appropriate training and 3) authorization from the owner of the asset for which access is being requested, the order of these 3 actions not being important. The Measures for R5.1 require that personnel risk assessments be completed before authorized electronic or authorized unescorted physical access is "authorized". PSE proposes that the wording in both bullet items in the Measure be changed from "access was authorized" to "access was granted". This would allow asset owners the ability to authorize access pending the successful completion of the PRA and/or training. This would also be more consistent with the wording in the requirement which indicates that the PRA must be performed prior to "granting" access.
1) In R6.4, PSE requests clarification around the intent of the requirement to track authorized access to the physical and electronic locations where BES Cyber System Information is stored. Is the requirement regarding physical location intended to include physical access to file servers hosting BES Cyber System Information in electronic format or is it intended to be limited to physical access to locations where BES Cyber System Information in stored in hardcopy format? 2) In R7.2, the

requirement is to revoke unnecessary access by the end of the next calendar day following a reassignment or transfer. As pointed out in the change rationale, the need for access may change over time. Often when an employee transfers there is a transition period where the employee may continue to require previous access to help support the old position. As currently written, there is no requirement to revoke the access if the determination of unnecessary access occurs after the next calendar day following the reassignment or transfer. PSE contends that a more effective control would result if the language of the requirement was changed to something similar to the following: "For reassignments, or transfers, review the individual's electronic and physical access and revoke any unnecessary access by the end of the next calendar day following the reassignment or transfer. Electronic and/or physical access required beyond that date is to be revoked by the end of the next calendar day following the determination that the access is no longer required." The Measures for this requirement should be updated accordingly. 3) In R7.3, similar to R6.4, clarification is needed regarding physical access to BES Cyber System Information. 4) In R7.5, PSE recommends changing "shared account(s)" to "BES Cyber System shared account(s)."
Yes
Yes
No
Yes
Yes
Comments: Recommendation to included cameras in the examples provided for "Locally mounted hardware or devices at the Physical Security Perimeter" because cameras tend to have the same characteristics as motion sensors, electronic lock control mechanisms, and badge readers. R1.6: The requirement states that the entity must have "controls that monitor each Physical Access Control System" but the measures reference documentation of controls that monitor the Physical Security Perimeter. PSE request clarity on whether the controls referenced in R1.6 are for the PACS or the PSP. R1.7: The requirement states that an alarm must be issued within 15 minutes of an unauthorized physical access being detected but the guidelines and technical basis state under methods to monitor physical access state that "…alarms must provide for immediate notification…" PSE suggests that the methods to monitor physical access to updated to reflect the 15 minutes defined in R1.7.
Yes
Yes
Yes
Yes
Yes
• Requirement 2, all sub-requirements: Applicable BES Cyber Systems and associated Cyber Assets - Change "Medium Impact BES Cyber Systems" to "Medium Impact BES Cyber Systems with External Routable Connectivity". Rationale: For non-externally routable or dialup systems the requirement, as currently written will create a large amount of compliance documentation without adding much security. • R1.1: Does the "where technically feasible" language imply that Technical Feasibility Exceptions (TFEs) are required when it is not technically feasible? • R2.1: Proposed - "A patch management program for tracking, evaluating, and installing cyber security patches and/or security updates for applicable Cyber Assets." • R2.2: Change 30 to 35 calendar days to assist with monthly patch cycles, increase efficiency, and align to other requirement's timeframe (ex: CIP-007, R3.3). • R3&4: Associated Protected Cyber Assets: Concern: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. • R4.1: Add the term "where technically feasible" to the requirement language and specify that a TFE would be required in these circumstances. Rationale: Not all systems can support the logging requirements in 4.1.1-4.1.4. • R4.2.1: Change "detected malicious activity" to "detected cyber security event". Rationale: not all security events are malicious, which the standard utilizes R4.3 to make the determination if the cyber security event logged was

malicious in intent. • R4.3: Change “Activate a response to detected event…” to “Activate a response to human-detected event…”Rationale: the requirements do not distinguish between the logging of an event by a system and when that event is detected by a person. A person may not see the event at the same time it is generated by a system, so the requirement should be clarified to reflect that the deadline for a response be tied to human detection of the logged event. • R4.3: Change “next calendar day” to “next business day” to accommodate off-hour staff coverage. • R4.5: Applicability - Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets”. Rationale: Clarifies that the logging reviews do not apply at the asset level. • R4.5: Change the wording to “Review a summarization or sampling of logged events, as deemed appropriate by the Responsible Entity, at a minimum…”. Rationale: It should be clear that the entity determines which logs should be reviewed or sampled, to avoid confusion during audits.
• R5.1, R5.4: Change “Medium Impact BES Cyber Systems” to “Medium Impact BES Cyber Systems with External Routable Connectivity or dial –up connectivity”. Rationale: Consistency with CIP-004 R6.2 • R5.2: Delete requirement since it’s covered by CIP-004 R6.2 • R5.3: Delete requirement and move rationale to CIP-004 R5 since it’s covered by CIP-004 R6 • R5.4: Change the wording from “Change default passwords…” to “Change known default passwords…”. Rationale: Manufacturers sometimes use system passwords that are not known to the entities. • M5.4: Remove the language from the first bullet “…when new devices are deployed”. Rationale: Time frames are covered elsewhere in the Standards
Group
PNM Resources
Michael Mertz
Yes
No
No
No
Yes
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
See comment submission from EEI.
See comment submission from EEI.
No
No
No
See comment submission from EEI.
No
No
No
No
No
See comment submission from EEI.
See comment submission from EEI.
Individual
Martin Bauer
US Bureau of Reclamation
Yes

Yes
Yes
Yes
Yes
Yes
No
The 30 day revocation does not adequately prevent malicious use. To fully mitigate potential for harm, accounts should be revoked much sooner.
Yes
Yes
No
Yes
Yes
The two different physical access controls requirement would not allow the use of Pin and Card systems. The Pin and Card system is a Two Factor authentication. The Pin data is on the Card which makes it part of the same system. If the intent is to allow Two Factor authentication as described in the Guidelines and Technical Basis the language in the requirement must clearly state it. To reiterate Two Factor authentication is not same as two different physical access controls. The language in the requirement read "utilize (insert "a two factor authentication") or two or more different…. .
Yes
Yes
Yes
Yes
Yes
Individual
Scott Harris
Kansas City Power & Light
No
No
No
No
Yes
No
No
R1.1: According to the Guidelines and Technical Bases Section “the Responsible Entity is not required to provide records that show that each individual received or understood the information.” This is not clearly stated in the requirement. Suggested change: 1.1 A security awareness program that, at least once each calendar quarter, makes available ongoing reinforcement of cyber security practices to the Responsible Entity’s personnel who have authorized electronic or authorized unescorted physical access to BES Cyber Systems. R2.1: An entities size will determine the necessity of multiple roles. For example, a company with 300 employees may require one role whereas a company with 30,000 employees will likely need several roles. This requirement should allow for these differences. Suggested Change: 2.1 Identify one or more roles. R2.2: According to the Rationale for R2, based on their role, some personnel may not require training on all topics; however, it is not stated in the Requirement. Also, according to the Guidelines and Technical Basis, training shall cover items appropriate to personnel roles and responsibilities. Suggested Change: 2.2 Cyber security training for

each role identified in 2.1 shall include one or more of the following topics appropriate to personnel responsibilities: R3.2: This requirement alone will dramatically increase time spent administering training because it requires staff to track numerous training dates as opposed to annual training dates. When combined with role-based training introduced in CIP-004-5, R2.1, it will require additional staff to manage. This places an undue burden on entities and Regional Entities. Suggested Change: 3.2 Require completion and documentation of the training specified in CIP-004-5, Requirement R2 once every calendar year. R4.2: Whereas Requirement 4.1 may slightly reduce the complexity and cost of background checks, this requirement complicates the task and will ultimately increase the cost of background checks as well as the amount of paperwork involved by forcing REs to document the reasons full seven year criminal history records checks were not performed. This task is unnecessary and adds little or no value to personnel risk assessment programs. I would suggest removing the second sentence in Requirement 4.2. Suggested Change: 4.2 Seven year criminal history records check including current residence, regardless of duration, and covering at least all locations where, during the seven years immediately prior to the date of the criminal history records check, the subject has, for six months or more: 4.2.1. resided; 4.2.2. been employed (if applicable); and 4.2.3. attended school (if applicable). R4.3 & 4.4: Examples of criteria in Requirement 4.3 & 4.4 or its Measures section are not provided. Suggested Change: Add criteria in Requirement or, at a minimum, add an “Evidence may include, but it not limited to:” section under its Measures to guide entities.
R6.5: The following statement in the Rationale for R6 on is not addressed in the Requirement or its Measures section: “If the results of quarterly or annual account reviews indicate an administrative or clerical error in which access was not actually provisioned, then the error should not be considered a violation of this requirement.” The inclusion of this statement in the Requirement in some manner would enable REs to find and fix this problem discovered during quarterly and annual audits rather than self-reporting them. Suggested Change: 6.5 Verify at least once each calendar quarter that individuals for which provisioning of authorized electronic access or authorized unescorted physical access in fact transpired have associated authorization records. R7 General: It is not clear that FERC’s order regarding “immediate” access removals be done that the requirements in versions 3 and 4 were found to be inadequate by FERC in addressing this concern. What was the motivation for the version 5 change in time frame from 7 calendar days to 1 calendar day? R7.1: In “Draft 1”, the SDT used the phrase “at the time” and in the Change Rationale section under Requirement 7.1 they stated that this requirement “specifies revocation concurrent with the termination instead of within 24 hours.” In “Draft 2”, the SDT allows the entity to initiate the process to revoke unescorted physical access and Interactive Remote Access upon the effective date and time of the termination action and complete the revocation within 24 hours after the effective date and time of the termination action. This is a significant improvement; however, in most circumstances still unrealistic. Suggested Change: 7.1 For all termination actions, initiate the process to revoke the individual’s unescorted physical access and Interactive Remote Access upon notification of the effective date and time of the termination action, and complete the revocation by the end of the next business day after the effective date and time of the termination action. R7.2: Although requiring revocation of access for reassignments and transfers “by the end of the next calendar day” is a more realistic time frame than the 24-hour time frame under Requirement 7.1, it gives entities little or no time to find and fix problems. Currently, entities have seven days to complete the process. Considering access revocation, especially in the case of transfers, is difficult and has many variables including the need for multiple supervisor approvals, limiting time to complete the process would dramatically increase the number of self-reports involving access revocation thereby creating an even more substantial paperwork nightmare for NERC. The SDT must reconsider the seven-day window allowed to revoke access under CIP-004-3, R4.2. Suggested Change: 7.2 For reassignments or transfers, revoke the individual’s electronic and physical access that the Responsible Entity determines is not necessary within seven days following the reassignment or transfer.
No
No
R1.1: Requirement statement seems to add to the scope of the applicability assets. Reword the requirements section. Current Applicable Statement: High Impact BES Cyber Systems Medium Impact BES Cyber Systems Suggested Applicable Statement: High Impact BES Cyber Systems and Associated Protected Cyber Assets with External Routable Connectivity Medium Impact BES Cyber Systems and Associated Protected Cyber Assets with External Routable Connectivity Current

Requirement Statement: All BES Cyber Assets and associated Protected Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP. Suggested Requirement Statement: Applicable Assets connected to a network via a routable protocol shall reside within a defined ESP. R1.3: Change the word “rational” to “reason”
Move examples cited into the measures for the three factors cited, leaving the requirement with the description of the factor. The measures would frame examples appropriate to each factor. The strike through wording needs to be moved to the measurements section. • Something the individual knows (including, but not limited to, passwords or PINs. User ID is not an authentication factor); • Something the individual has (including, but not limited to, tokens, digital certificates, or smart cards); or • Something the individual is (including, but not limited to, fingerprints, iris scans, or other biometric characteristic).
No
Yes
Yes
R1.3: This requirement requires more than one access control system that can uniquely identify a person for facilities in the High category. This requirement is will costly to implement and does not recognize defense in depth, or organizational and procedural controls that can be implemented in the temporary absence of a control. Recommend the following change to recognize the layering of defenses: Where technically feasible and for facilities with one layer of physical protection, utilize two or more different physical access controls to collectively allow physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access. R1.4: It is not clear that requirement R1.4 is for monitoring of the entry points into the Physical Security Perimeter (PSP) and not monitoring the equipment that monitors the entry points into the PSP. Recommend the following for clarity: Have controls that monitor the Physical Security Perimeter twenty four hours a day, seven days a week (with 99.9% availability), for unauthorized access into a Physical Security Perimeter.
No
No
No
No
No
R1.1: Applicable BES Cyber Systems and associated Cyber Assets: Clarify how “Associated Protected Cyber Assets” is a modifier to the “High Impact BES Cyber Systems” and “Medium Impact BES Cyber Systems with External Routable Connectivity” rather than an independent set of assets. One option is to add “and Associated Protected Cyber Assets” to each of the High and Medium categories in this requirement. Additional clarification should also be available with respect to how ports are defined as “needed.” Suggested change: “For applicable Cyber Assets with logical network ports, enable only approved logical network accessible ports, including port ranges or services where needed to handle dynamic ports.” R1.2: This control is redundant and is covered through other physical security related requirements. All medium and high impact systems should already be protected. Signage is not going to be helpful in addition to the existing screening, escorting, barrier placement, physical access logging, and monitoring controls in place. R2.1: The measures should include better guidance as to what is considered to be an appropriate source of security patch information. Are entities able to use third parties for patch information instead of manufacturer-specific patch release information? R2.2: Change 30 to 35 calendar days to assist with monthly patch cycles and increase efficiency. R2.3: There is some confusion over the ability to revise an existing plan when new information comes to light. Recommend changing R2.3 to, “For applicable patches identified in Part 2.2, create a dated plan or revise an existing plan within 35 calendar days of the initial evaluation completion or identification of need to revise an existing plan. The plan shall include the Responsible Entity’s planned actions to mitigate the vulnerabilities exposed by each security patch and a timeframe to complete these mitigations.” R2.4: The current wording implies that the plan must be implemented within the timeframe specified in the original plan. Recommend change to, “Implement each plan created in Part 2.3, or a successfully revised version of the plan, within the timeframe specified in the plan, except for CIP Exceptional Circumstances.” R3: Associated Protected Cyber Assets: The inclusion of this category in the requirements for Malicious Code Prevention and Security Event Monitoring implies that these requirements apply to every device in the category. This departs from the goal of applying

these controls at the system level. Suggestion: Clarify that these requirements do not apply to all assets individually, by removing the category, or modifying the requirement. R3.3: Recommended that “with external routable protocol” be added to the applicable section. R4.1.4: Remove 4.1.4 – it will be difficult to detect and log for unspecified malicious activity and impossible to prove we are logging malicious activity if we do not have any malicious activity. R4.2: The sub-requirements imply that entities will be required to constantly prove the negative with regard to malicious activity. There are many ways of detecting malicious activity or the failure of a logging activity, and some of them cannot be automated to allow for alerting in a manner that would satisfy the requirement. Recommend, “Generate alerts for security events that the Responsible Entity determines necessitate a real-time alert.” R4.3: This will require Entities to make increased financial and manpower investments in efforts to be compliant. One calendar day is unrealistic and unattainable in most circumstances. Change next calendar day to next business day, “Activate a response to alerts generated in compliance with R4.2 by the end of the next business day.” In the Measures: Change “attestation” to “documentation” for clarity. R4.4: Applicability is confusing because the requirement states “BES Cyber System” which does not include these associated systems. Remove the three “Associated…” systems/assets from the applicability section. R4.5: Applicability is confusing and suggest change to requirement for clarification, “Review a sample of logged events at a minimum every two weeks to confirm that logs are being generated as expected.” Consolidate “High Impact BES Cyber Systems” and “Associated Protected Cyber Assets”, by changing the wording to “High Impact BES Cyber Systems with Associated Protected Cyber Assets” Remove “Associated Physical Access Control Systems” and “Associated Electronic Access Control or Monitoring Systems”
R5.4: Clarify that default passwords that are unchanged will require changing according to R5.6. R5.5: Attestations in the measures section should be removed. R5.6: Add where technically feasible or “unless the BES will be negatively impacted” verbiage to the end of the requirement. R5.7: Current language implies that generating alerts for unsuccessful login attempts is not a method of “limiting the number of unsuccessful authentication attempts.” This could be interpreted to mean that a TFE should be generated when an entity has established a failed login alerting threshold but not implemented other means to limit unsuccessful attempts. The end result would require entities to fill out quite a bit of paperwork to account for all of the TFEs. A description of “alerting” or other methods for “limiting” the number of attempts can be placed in the measures. Recommend, “Limit the number of unsuccessful authentication attempts after a threshold of unsuccessful login attempts, or document other means by which the number of unsuccessful authentication attempts can be minimized.”
Individual
Darcy O'Connell
California ISO
No
No
No
Yes
Yes
No
No
CIP-004-5 R1 M1. Change “but not limited to” to “but is not limited to” CIP-004-5 R2 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based. R2.1 - Change “identification of each role” to “identification of roles” required for BES cyber access. Consider removing R2.10, it is difficult to determine the intention of this requirement. It does not add anything that is not covered in 2.2 through 2.9. CIP-004-5 R3 - Remove “role-based cyber security training” to training based or tailored to job function. Role-based seems that it is inferring that training should be based on permissions or that access should be role based.
CIP-004-5 R6 Part 6.6 - Remove Measure “2. A summary description of privileges associated with each group or role;“ CIP-004 R6 – Part 6.1 – 6.1.3 states “access to the physical and electronic locations where BES Cyber System Information is stored by the Responsible Entity.” The wording should be cleaned up for physical location. i.e. a janitor has access to a data center therefore he has physical access to BES Cyber System Information because the data is stored on a SAN in the data

center. CIP-004-5 R7 - R7.2 For reassignments and transfers suggest changing the duration from one calendar day to 30 calendar days as is prescribed for terminations in Parts7.4 and 7.5. A termination is a higher risk vs. a transfer.
No
The Measures in Part 1.7 are prescribing an Intrusion Detection System however such system is not prescribed in a requirement. The references to an IDS should be removed. Other systems and tools can be used to detect malicious communication other than an IDS. Requiring encryption in CIP-005 R2 Part 2.2 will not allow an IDS to detect malicious communication. Especially if ssh is used between the intermediate device and the cyber asset.
No
No
Yes
CIP-006 R1 – Parts 1.4 and 1.6 change “Have controls” to “Have control(s)” Parts 1.5 and 1.7 remove reference to “BES Cyber Security Incident Response Plan” since this is a Physical Incident and not cyber. Part 1.5 Revert to the wording that was in the previous draft of CIP Version 5. CIP-006 R2 - Measure in Part 2.2 appears to be a copy and paste error. Suggest revisiting Measure 2.2 as it does not align with the requirement.
No
Yes
No
No
No
CIP-007 R1 R1.2 Suggest replacing the requirement with a requirement for the Responsible Entity to implement a policy regarding the use of physical ports. CIP-007-5 R3 - Part 3.1 strike the word “deter” in the requirement. Not sure how you deter malicious code. Part 3.2 Measures should be limited to response actions for detection malicious code. Remove bullets 2 and 3 for the measures. Part 3.3 The sentence structure for the requirement is awkward. Please reword the requirement for easier read. CIP-007-5 R4 - R3 and R4 one states malicious code and the other says malicious software. Suggest changing to malicious code for consistency. Part 4.1.4 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2.1 suggest removing this part. Otherwise, define what is malicious activity. This is subject to interpretation. Malicious activity requires analysis and is not something that can be logged. Part 4.2 remove “real-time”. Is real-time when the event is received by a tool or when the event occurred on a cyber asset. Some events may only be processed by a tool on a daily basis (batch). Part 4.3 standardize with CIP-006 R1.6 in regards to availability and keeping records for outages. Is the requirement in regards to the security monitoring logging capability or in regards to a cyber asset not logging? Part 4.5 should only pertain to where automated processes and alerting are not possible.
Part 5.1 remove the word “all” or be specific to scope. Define what is meant by “user access”. Provide better examples for measures in order to provide guidance for intention of the requirement. Reword requirement to “Enforce authentication of interactive user access to Applicable BES Cyber Systems and associated Cyber Assets, where technically feasible.” or change to require authentication of accounts. Part 5.2 suggest rewording to “The CIP Senior Manager or delegate(s) must authorize enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s). “ Part 5.3 for the measure reword to “Evidence may include, but is not limited to, listing of shared accounts and the individuals who have authorized access to each shared account.” Part 5.4 reword to “Change default passwords, where technically feasible, unless the default password is unique to the Cyber Asset.” Part 5.5.1 reword to “Password length that is, at least, eight characters or the maximum length supported by the Cyber Asset; and” Part 5.5.2 reword to “Minimum password complexity that is at least three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non-alphanumeric) or the maximum complexity supported by the Cyber Asset.” Part 5.5 Remove Measure around attestations. Additionally, some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states “Documentation of the registered entity’s procedural solution and training

program to educate its affected personnel on its procedural solution." Part 5.6 Remove Measure around attestations. Additionally, some organizations are dependent on unions that will not allow for attestations by union members. Add measure that states "Documentation of the registered entity's procedural solution and training program to educate its affected personnel on its procedural solution." Part 5.7 reword to "Where technically feasible, limit the number of unsuccessful authentication attempts or generate alerts after a threshold of unsuccessful login attempts." Should there be a recommended minimum for both?
Group
BC Hydro
Patricia Robertson
Yes
No
Yes
No
Yes
Yes
No
1) Requirement R2.5: question - is the Registered Entity expected to track the names of all individuals who have undertaken training related to the visitor control program? If yes, what evidence will need to be provided that this training was completed? 2) Requirement 4.3: "Process or criteria used to evaluate personnel risk assessments to determine when to deny authorized access". Access decisions will be based on a case-by-case basis and on the facts surrounding each; as such, defining such a process that will be adhered to each and every time may be difficult to define. Recommend changing the word "process" to "guideline"
Requirement 7: for conditions where access is to be revoked by "next calendar day" it is requested that this time period be restated to "next business day" to account for weekends and statutory holidays; the time period in which to revoke access would also be based on risk
Yes
Yes
No
No
Yes
1) Requirement 1.4: I agree with the Registered Entity looking to achieve high availability (HA) for physical access control (systems) but 99.9 % seems excessive; it is unclear as to how the Registered Entity is expected to evidence the 99.9% HA; there will be legitimate scenarios, such as patching the OS, where it may be difficult to meet the 99.9% HA as there are scenarios where the system is down very briefly for maintenance, such brief time periods where the system may be down, for example a reboot to allow installation of patches (what is there are a large number of patches to be installed throughout the year?).2) Requirement 1.7: for clarification, an alarm is required to be generated within 15 minutes resulting to a potential PSP breach, not the response. It is not always possible to initiate a response for remote unmanned sites where someone can be on site within 15 minutes, it may take hours, to investigate a potential PSP breach 3) Requirement 1.9: clarification is required that only the most recent 90 days of logs need to be retained by the Registered Entity as opposed to being required to demonstrate that for any day within the audit period 90 days of data was retained. 4) Requirement 2.3: clarification is required that only the most recent 90 days of visitor logs need to be retained by the Registered Entity as opposed to being required to demonstrate that for any day within the audit period that 90 days of data was retained.
Yes
Yes
Yes
Yes

Yes
Group
Hydro One
Sasa Maljukan
No
No
Yes
No
Yes
Yes
No
Recomend removing word “potential” from R2 part 2.7 since an incident is determined to be real or potential only during the follow up investigation R4, part 4.2 it pelase include wording to state that PRA should include all bulleted items (4.2.1 through 4.2.3) to avoid confusion. Privious version of R4 part 4.3 had exclussion for laws or collective barganing agreements. Pelase add the exclussion or explain why the exclussions were dropped.
No
No
Recommend removing “, but is not limited to, ” from R1 Part 1.1 since the Measure’s scope already includes all of the possible Cyber Assets We understand that Measures should not dictate Requirements. If correct, then how can CIP- 005 R1 Part 1.5’s Measure specify “intrusion detection system” when the Requirement does not specify a technology. Also specifying a technology may prevent a newer, better technology from being used until the Standard is updated. Recommend changing R1 Part 1.5 from “intrusion detection system” to “detection system” Request for clarification on how the math for R1 is done in the VRF/VSLs
Request clarification on R2 Part 2.1 – can the Intermediate Device can be on the ESP? In other words, can the Intermediate Device also be an EAP? Recommend changing R2 Part 2.3 from “Factors must be at least two of the three following categories” to “Multi-factor include, but are not limited to” which allows future technology without a Standards update
No
Yes
No
Recommend changing the testing in R3 Part 3.1 so that the High Impact BES Cyber Systems are tested every 24 months and Medium Impact BES Cyber Systems with External Routable Connectivity are test every 36 months
Yes
No
No
No
No
For R2, request clarification if the SDT’s intent is that the following timeline will be compliant or not? 1) on 5/1/2012 the patch is identified; 2) by 6/1/2012 complete the assessment for applicability (30 days); 3) by 7/1/2012 the plan is developed and defined for testing plus implementation (30 days); 4) per the plan, testing completed by 9/1/2012; 5) per the plan, patch deployed by 10/12/2012; 6) on 10/30/2012 patch fails (through no fault of testing); 7) emergency patch back out on 11/1/2012; 8) per plan, develop mitigation plan by 12/1/2012 (30 days); 9) per original plan, mitigation testing completed by 2/1/2013; and 10) per original plan, mitigation patch deployed on 3/12/2013 Recommend changing R3 Part 3.3 so that Medium Impact remote locations with no external connectivity (isolated networks) have more than 35 days Suggest changing R4 Rational from “(1)

immediate detection" to "(1) real time detection" to be consistent with Part 4.2 Request clarification on R4 Part 4.1.1. The CIP Standards expect "deny by default" firewall rule which results in dropping offending packets such that there is nothing to log. How can the Registered Entity meet Part 4.1.1 criteria of logging failed access attempts at the EAP? Recommend removing "malicious" from R4 Part 4.1.4 since "malicious" is determined after the fact and Parts 4.1.1, 4.1.2 and 4.1.3 capture the events that may be malicious • R4.5 – Bi-weekly manual reviews of sampling of logged events –what is considered a "sampling of logged events"? Is this a percentage of logs received (on average)? Who make the determination that an appropriate number of logs have been reviewed ? how will auditor determine that a manual review had been completed? What is the ultimate value of a manual review? For R1 as written, recommend that missing one port is too high since the PSP is the first layer of defense. Missing one physical port should not be a Severe VSL. Recommend this is a Low VSL. Recommend increasing percentages from Low – Moderate – High – Severe Recommend that the number of assets should be another differentiator for R3's Low – Moderate – High – Severe Recommend that the difference between R4's Low – Medium – High – Severe should be number of assets with two weeks throughout Recommend that R4 should start with a Low VSL and use the number of assets combined with the number of accounts as a difference between Low – Medium – High - Severe
Request clarification on R5 Part 5.7. Does the technical feasibility apply to both "the number of unsuccessful authentication attempts" and "generate alerts after a threshold of unsuccessful login attempts" or only the "authentication attempts?"