Individual or group. (112 Responses)
Name (84 Responses)
Organization (84 Responses)
Group Name (28 Responses)
Lead Contact (28 Responses)
Question 1 (0 Responses)
Question 1 Comments (93 Responses)
Question 2 (0 Responses)
Question 2 Comments (93 Responses)

Individual
Brian S. Millard
Tennessee Valley Authority
Please see comments provided previously for CIP Version 5 Draft II standards CIP-002-5 through CIP-011-5, definitions, and implementation plan. Draft III Comments: CIP-002-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-002-5 R1 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-002-5 R2 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-004-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-004-5 R2.2 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-004-5 R3 - The subrequirements are unclear due to grammar. CIP-004-5 R5 - For transfers within the organization/entity, the change of the time required to revoke access from 7 calendar days to 1 calendar day adds no reliability benefit. CIP-005-5 R2.1 - Need clarification on protections to be afforded to an "intermediate device". CIP-005-5 R2.2 - It is reasonable to include traffic between the "intermediate device" and device(s) within the ESP to be in scope of CIP, as it traverses an EAP. To include traffic that originates beyond the "intermediate device" does not afford additional protection to the systems essential to the reliable operation of the BES. CIP-006-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-006-5 R1.6 - The definition of PACS includes badge readers which are on the unsecured side of a PSP, and therefore access to them cannot be controlled in the manner required by R1.6. CIP-006-5 R1.7 - The definition of PACS includes badge readers which are on the unsecured side of a PSP, and therefore access to them cannot be controlled in the manner required by R1.7. CIP-006-5 R2.1 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-006-5 R2.2 - CIP Exceptions Circumstance clause should be removed as it applies to numerous parts and is stated at the policy level. CIP-007-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-007-5 R1.2 - No clarification is made regarding physical I/O ports that are externally accessible. For example, most servers have PCI slots, CPU slots, memory slots, etc, which are physical I/O ports. As the standard is currently written, it would seem organizations need to disable these ports. Additionally, the language “console commands” is too ambiguous. CIP-007-5 R2.3 - "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to “create a dated mitigation plan” or “revise an existing mitigation plan” will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to “Develop dated implementation plan” without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability. CIP-007-5 R2.4 - "Available actions to entities should include: 1) Apply the patches 2) Develop dated implementation plan 3) Create/revise existing mitigation plan". In many cases, patches will be applied, but outside of a 35 day period to accommodate outage schedules for optimizing reliability and availability of systems. In many cases, when an applicable patch is provided by a vendor, there may be no additional mitigation implemented during the time from patch availability until installation. Requiring entities to “create a dated mitigation plan” or “revise an existing mitigation plan” will result in a paperwork exercise and yield no reliability or security benefits for the affected cyber assets. Adding an option to “Develop dated implementation plan” without requiring a mitigation plan to be created/modified permits entities to apply resources to application of patches and optimizing reliability. CIP-007-5 R4.1.3 - The requirement for malicious code prevention methods to log is contained in the R3.2 subrequirement. Remove requirement 4.1.3 as it is redundant. CIP-007-5 R4.2 - 4.4 - The requirements and subrequirements have become less clear than previous revisions of the CIP standards. It is unclear if R4.4 replaces the previous monitoring requirements in their

entirety, or represents an additional manual sampling action that occurs outside of a primary monitoring process which may be automated. Please consider modifying the R4.2-4 subrequirements in their entirety to make it clear to RE's which logging is required, how logs should be monitored (manual, automated, or both), and what actions are required in the event of an interruption in logging. CIP-007-5 R4.4 - It is unclear if this replaces the previous monitoring requirements in their entirety, or represents an additional manual sampling action that occurs outside of the primary monitoring process. CIP-008-5 R3.2 - Update 60 day requirement to 90 days to be consistent with R3.1. CIP-009-5 R1.5 - Need clarification - the example provided seems like it would delay the recovery process, although it is stated that data preservation should not impede recovery. CIP-009-5 R2.3 - Discrepancy regarding the time frame for testing has been identified as 12 months In the Implementation Plan for V5 CIP Cyber Security Standards-section 6, and in section 7 as 24 months- which is correct? CIP-009-5 R3.2 - Update 60 day requirement to 90 days to be consistent with R3.1. CIP-010-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-010-5 R1 - Inconsistent time frame for completion of configuration control activities. This introduces the possibility of confusion in completing activities required for other CIP reliability standards. CIP-010-5 R2 - Inconsistent time frame for completion of configuration control activities. This introduces the possibility of confusion in completing activities required for other CIP reliability standards. CIP-010-5 R3.2 - What is the time period for documenting results? CIP-010-5 R3.3 - An effective active vulnerability assessment may not be possible on a system prior to connecting it to its network as many of the applications that run on a device may not function outside the presence of other peripheral devices (ie, SCADA client application won't launch without SCADA Master connectivity available). Therefore, any active vulnerability assessment would probably be limited to an AV scan and account review, at most. Both of which could be effectively controlled through the use of solid imaging/deployment procedures. Modify language so that it is not required prior to adding the asset to the production environment. CIP-010-5 R3.4 - What is the time period for documenting results? CIP-011-5 - Definition of EACMS is inconsistent with definition provided in "Definitions of Terms Used in Version 5 CIP Cyber Security Standards". This could result in misidentification, misapplication or inconsistent application of standards. CIP-011-5 R1.2 - Clarify "transit"; is it in regards to physical or electronic transit? Definitions: There is still no clear definition for BES Cyber System. Definition provided for EACMS is inconsistent with definitions provided in the "Background" section of the CIP 002, 004, 006, 007, 009, 010, and 011 standards.

Group

Colorado Springs Utililties

Shannon Fair

No Comments for any of the NERC CIP requirements

N/A

Group

ACES Power

Jason Marshal

(1) We thank the drafting for improvements to the draft standard. However, we still believe there is room for more improvement before voting affirmative for CIP-002-5. We are concerned that the impact of the standards on small TOPs is not commensurate with their impact on reliability and is not consistent with BA and GOP criteria. Per criteria 1.3 and 2.12, all TOP control centers and backup control centers will be either High Impact or Medium Impact regardless of how small they are. Criteria 2.11 and 2.13 establish a 1500 MW floor for GOP and BAs. Why would similar floor not be established for the TOP? Is control of generation somehow less important than control of transmission? What if the BA and TOP are the same company? We have a member that has approximately 300 MW of load in their BA and their highest transmission voltage is 161 kV for their TOP. A Medium Impact assessment of their control center simply does not reflect the minimal reliability impact that this BA has on the Bulk Electric System. (2) CIP-002-5 through CIP-011-1, Applicability sections 4.1.2.4 and 4.2.1.4: Please strike "and group of Elements" as it is redundant with Cranking Path. By definition, the Cranking Path is "a portion of electric system that can be isolated and then energized to deliver electric power from a generation source". Cranking Path will include the "group of Elements meeting the initial switching requirements". Thus, the inclusion of this language is unnecessary and will only contribute to ambiguity. Distribution Providers will be forced to question if the drafting team intended to include something above and beyond the Cranking Path. (3) CIP-00-5 R1 and associated VSLs: The requirement uses the term "assets" and the VSL uses the term "BES assets". Both the requirement and VSL should consistently use that same term. (4) CIP-002-5 R1 Part 4 and Attachment 1 Criterion 3.4: Part 4 and Criterion 3.4 need to be modified to use language consistent with the EOP-005-2, EOP-006-2, and the Applicability section 4 of the CIP-002-5 through CIP-011-1 standards. Please change "blackstart generators" to "Blackstart Resources". Also, please change "substations in the electrical path of transmission lines" to "Cranking Path". Blackstart Resources and Cranking Path have specific meanings and are consistent with other standards. Use of terms that are not defined when specifically defined terms exists creates ambiguity in the meaning of the standard. It will cause registered entities to question if something else is meant by these terms. Furthermore, "substations in the electrical path of transmission lines" would not be consistent with the Applicability section regarding Distribution Providers since they will not have transmission lines. (5) CIP-002-5 R1.1 through R1.3 and

R2.1 and R2.2: Use of sub-requirements is inconsistent with the NERC filing in which NERC committed to using numbered or bulleted lists and which was approved by the Commission on May 19, 2011. Please change accordingly. (6) CIP-002-5 R2.1: Please modify "Review (and update as needed) the identification" to "Review the identification and update it if there are changes identified". Otherwise, it implies that the registered entity is to conduct additional reviews and updates whenever there might be a change which could compel the registered entity to continuously review its identification from Requirement R1. (7) CIP-002-5 Attachment 1: Please clarify "planning horizon of more than one year". Does this mean that it occurs in the planning horizon in multiple years (i.e. 2015 and 2016) or does it mean it covers any single planning year that is at least 12 months from the operating day? The Guidelines and Technical Basis don't offer any clarification because they use slightly different language ("of one year or more"). We suggest that the drafting team consider using the term "Year One" as it provides more clarification and there really is no need to look beyond the first year of the Near-Term Transmission Planning Horizon which is also a defined term. If a generation Facility is identified beyond Year One as required to avoid an Adverse Reliability Impact per Criterion 2.3, it is entirely possible that the planning assessment will change and obviate the need for the generator to avoid the Adverse Reliability Impact. (8) CIP-002-5 Attachment 1: Please change "System" to "system" in Criterion 2.9. It is not used consistently with the NERC Glossary definition. (9) CIP-002-5 Attachment 1: Please add a qualifier to Criterion 3.1 that clarifies it only applies to BA and GOP control centers. All RC and TOP control centers will have been included in Medium and High Impact through criteria 1.1, 1.3, and 2.12. (10) CIP-002-5 Attachment 1: In criterion 2.10, please strike "or group of Elements". Use of Elements is not consistent with the NERC definition. Elements are not typically components of a control system. Use of Elements here implies they are part of the control system for automatic Load shedding. (11) In the Guidelines and Technical Basis section beginning on page 17 and ending on page 22, we continue to believe the functional entities should be removed from the reliability operating services. Many of the reliability operating services are not attributed to correct functional entities. For instance, under ability to implement load changes for demand response under the Balancing Load and Generation section is incorrectly attributed to the TOP. The TOP will have nothing to do with Demand Response as this is a market function. Please see our previous comments for more examples. (12) In the Guidelines and Technical Basis section on page 21, the Managing Constraints section inappropriately attributes ATC to managing constraints. ATC is about selling transmission service and has nothing to do managing constraints. Transmission service is a right to use the system that may never be utilized and cannot itself cause a constraint. (13) On page 25 of the Guideline and Technical Basis in the fourth paragraph, please strike "which coordinates actions necessary for the implementation of these plans by affected parties". The RRO plays no such role. The coordination is performed by the Transmission Planner or the Planning Coordinator. Furthermore, inclusion of this language before the phrase "usually in the form of a formal agreement and/or contract" makes it sound like the RRO is negotiating the contract which they are not and cannot because they are not a party to such contracts. Please also note that RRO is not an appropriate reference for Regional Entity. (14) Please reword the second sentence in the last paragraph on page 25 regarding criterion 2.9. It is a run-on sentence and its meaning is not clear. (15) CIP-003-5 is dependent upon CIP-004 through CIP-011 being approved. We are concerned with the implementation of the standard if any of the other standards do not pass. (16) While we agree that CIP-003-5 does not need to require implementation, we suggest combining the implementation of security procedures in CIP-004 through CIP-011 that have actions associated with them. (17) CIP-003-5 Requirement R1 only applies to high impact and medium impact BES Cyber Systems. The requirement or measure should clearly state that low impact BES Cyber Systems do not apply to R1. (18) CIP-003-5 Requirement R2 is confusing in regard to low impact BES Cyber Systems. There is a sentence without any requirement or sub-part assigned to it that states an inventory, list or discrete identification is not required. Are low impact systems applicable to R2? Was this sentence meant to be part of the measure? Regardless of those questions, this sentence should be written in active voice, e.g., "Low impact BES Cyber Systems or low impact BES Cyber Assets are not required to have an inventory, list, or discrete identification." This sentence is confusing and does not tie into an obvious area of R2. We suggest clearly identifying the role of low impact BES Cyber Systems and Assets and the applicability to R2. Furthermore, it is not written consistently with CIP-002-5 R1.3 which is the first instance of trying to indicate an inventory is not required for low impact BES Cyber Systems. We suggest if it is retained it should be written consistently. (19) CIP-003-5 Requirement R2, parts 2.1 through 2.4, the SDT should consider combining these sub-parts. Awareness, security controls, access, and incident response are already listed in R1, part 1.3 and, therefore, this additional requirement is potentially redundant, unnecessary, and poses a risk of double jeopardy. If a responsible entity already addresses these items in cyber security policies that address high and medium impact BES Cyber Systems per R1, it should be free to apply all or parts of these same cyber security policies to low impact BES Cyber Systems per R2. Please clarify R1 and R2 so that this potential for double jeopardy is eliminated. (20) CIP-003-5 Requirement R2, part 2.3, for low impact BES Cyber Systems, we still have concerns about the modified language, "electronic access controls for external routable protocol connections and Dial-up Connectivity." We believe that the revised language also provides too much detail for these policy topics. The modification does not support the additional language and the responsible entity is in the best position to determine how to design its low impact BES Cyber System program based on the various differences that were mentioned in the previous drafts. (21) CIP-003-5 Requirement R3, does the CIP Senior Manager need to be a different person from the "high level official" that designates the CIP Senior Manager? There are instances where the CIP Senior Manager is going to be the same person in charge of the entity's compliance program. The SDT should consider what types of changes trigger documentation – "any change" could require documentation any time that CIP Senior Manager changes their title, gets promoted, etc. Regardless of a person's

position within the company, the designation of from the high level official would also put that person in the role of CIP Senior Manager. "Any change" should be only when that person leaves the organization or is no longer in the role of CIP Senior Manager. (22) CIP-003-5 Requirement R4, why does the Responsible Entity need to implement internal controls on delegating authority? The measure does not provide examples of internal controls, it only provides the end-state – a dated document showing the delegation. We recommend reducing the amount of words in R4. It is wordy and confusing. Why not use the language in the FERC Order or the Blackout Report ("clear lines of authority and ownership for security matters"). This would include delegations of authority. R3 and R4 could be combined and internal controls are not necessary for a result-based requirement. (23) If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. In the phrase, "These delegations shall be documented, including the name or title of the delegate, the specific actions delegated,…" authority for specific actions should be delegated, not the actions themselves (use "the specific actions for which authority is delegated"). (24) CIP-004-5 Requirement R1, "reinforcement" is vague, ambiguous, and opens the door to subjectivity and misinterpretation. Does the SDT intend to have a quarterly training, or a quarterly newsletter, or just a poster on the wall or an intranet posting? These are all options in CIP-004-5 Table R1. We suggest clearly defining what is intended with Requirement R1. If the SDT is planning to use internal controls for the majority of the CIP standards, the Responsible Entity should be the one to define what is appropriate for "reinforcement." We suggest either revising the language or removing it from the standard. There are already several standards that handle training and if the objective of this requirement is to have a poster on the wall that is administrative in nature. Please do not add requirements to the CIP standards that would be subject to Paragraph 81 retirement. (25) Requirement R1 (security awareness) looks like a purely administrative requirement. The risk to the BES because a quarterly awareness bulletin was not sent would be de minimis. If this requirement remains, it should be made clear that it is not a zero defect requirement. (26) CIP-004-5 Requirement R2 should be the only requirement for CIP-004-5. If the new paradigm for NERC is to shift to internal controls, then the SDT should not have any other requirements other than the overarching R2. The Training Content in CIP-004-5 Table R2 is too prescriptive and should be moved to the measures. If the Responsible Entity must create a Cybersecurity Training program, then the Responsible Entity should be able to determine the controls that ensure proper training is delivered to the appropriate personnel. (27) CIP-004-5 Requirement R2, Table R2, Part 2.2 is needs to be modified. As it is currently written, it literally says that access cannot be granted prior to completion of training. For newly responsible entities this language would be problematic because access has already been granted to existing employees before the standard is applicable. We suggest some language should be added to clarify that the training should be completed either prior to granting access or by the time the requirement applies to the responsible entity. . (28) The original rationale for the seven-year timeline was based on the Fair Credit Reporting Act (FCRA). We do not believe that the FCRA is a sound technical justification for criminal risk assessments. We suggest the SDT modify the timeline to 10 years to align with other governmental standards and practices. (29) CIP-004-5 Requirement R4, Part 4.2, requiring a validation of authorized access each quarter is reasonable but sounds a lot like an internal control. Thus, we are confused about what constitutes internal controls and what constitutes requirements. In the rationale for R4, the SDT states that administrative and clerical errors should not be a violation, and we agree. The Responsible Entity is in the best position to determine its internal practices and controls. We strongly suggest that the SDT remove Part 4.2 from Table R4 and provide it as an example of an internal control that the CEA would expect to see. This would allow the entity to determine the proper timeline for reviews by implementing controls that are based individual facts and circumstances. (30) CIP-004-5 Compliance Section, the evidence retention for verifying access should be less than the audit cycle (which is three years for BAs and TOPs), especially if the SDT plans to keep the quarterly reviews to verify that access has been properly removed. This is another administrative burden to maintain the documentation and we suggest reducing the evidence retention period to 15 months. (31) CIP-005-5, Requirement R1, Guidelines and Technical Basis, page 20: What is the rationale for standalone networks that have no external connectivity to other networks must have a defined Electronic Security Perimeter (ESP)? The risk basis for these networks that have no external connectivity are relatively low and therefore, do not need to be included in the standard. (32) CIP-005-5, VSL R1. The language in the VSL should match the same language and logic as R2. For example, the Responsible Entity should have a low VSL for not having a sub-part in its documented process, medium for not implementing one of the applicable items, high for not implementing two applicable items and severe for not implementing three applicable items. This would result in a more consistent application throughout the standard. (33) CIP-006-5, Requirement R1, Part 1.5 and Part 1.7. Combine the two requirements by adding Physical Access Control Systems (PACS) to Part 1.5 instead of separating the three assets into two requirements and measures since they are the same. It should read: Requirement: Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter and Physical Access Control System to the personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of detection. (34) CIP-006-5, R1.9 and R2.3: These are data retention requirements and should not be requirements of the Standard (35) In CIP-007-5 Requirements 3.1 - Deploy method(s) to deter, detect, or prevent malicious code, Requirements 3.2 - Mitigate the threat of identified malicious code and Requirements 3.3 - For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns. These three requirements do not have any timeline for action. Does the auditor audit when the activity occurred and audit only that a process is created and executed as per the registered entities procedure / process? (36) CIP-007-5 R4 – Security event monitoring does not state any requirements as to when the security events (Part 4.1: Log Events

and Part 4.2: Event Alerts) are to be reviewed, escalated and mitigated. The requirements state that the BES Cyber System be configured for event monitoring and alerts. Are there any requirements for immediate action from the IT Security personnel for detected failed access attempts, failed login attempts or specific event alerts? (37) CIP-007-5, R4.3This is a data retention requirements and should not be requirements of the Standard (38) In the Guidelines and Technical Basis Section for CIP-007-5 R4, it states, "Refer to NIST 800-92 and 800-137 for additional guidance in security event monitoring." Are these references to NIST the guiding principles and documentation for the development of the RSAWs and auditing of this requirement? (39) CIP-007-5 Part 5.1 and CIP-005-5 Part 2.3 – How do these parts differ? Both appear to require authentication of Interactive Remote Access sessions. (40) CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard. (41) In CIP-009-5 R2.2: How does a registered entity test a representative sample of information if per R2.1 they performed a paper drill? What sample of information is appropriate to ensure that in the information is useable and is compatible with current configurations from a paper drill? (42) Removal of BES before Cyber Asset in CIP-010-1, Requirement R1, Part 1.1 has the impact of greatly expanding the requirement. By definition a Cyber Asset is any "programmable electronic device." Thus, computer systems that have absolutely no impact on the Bulk Electric System could be pulled into the requirement. We recommend not only adding BES back to Cyber Asset but also clarifying that the requirement only applies to applicable BES Cyber Assets. Thus, we suggest replacing "Cyber Asset" with "applicable BES Cyber Asset" throughout Part 1.1 and its associated measure. (43) The timeline established for CIP-010-1, Requirement R1, Part 1.3 conflicts with some of the timelines established in CIP-005-5 and CIP-007-5. For example, Part 3.3 in CIP-007-5 requires an update of "malicious code protections" at least once every 35 days. CIP-010-1 R1 Part 1.3 requires updates to the baseline configuration within 30 days which would also included updating "malicious code protections". We suggest removing CIP-005 and CIP-007 as a reference to eliminate this issue. (44) CIP-010-1, Requirement R1, Part 1.3 presents opportunities for double jeopardy by including references from CIP-005 and CIP-007. If a change to the ports configuration is made but documentation from CIP-005 and CIP-007 is not updated, CIP-010-1 R1, CIP-005 and CIP-007 could all be violated simultaneously. (45) CIP-010-1, Requirement R1, Part 1.4.1, which cross-references CIP-005 and CIP-007 is loosely written and is open to subjectivity. The determination of security controls that "could be impacted" by the change does not reference any level of probability that the controls would be impacted, so any remote possibility could subject a Responsible Entity to a potential compliance violation. We suggest modifying Part 1.4.1 to eliminate cross-referencing other standards to avoid confusion and increase the probability for impacts by the change. A possible modification could state, "Prior to the change, determine cyber security controls that have a high likelihood to be impacted by the change." (46) CIP-010-1, Requirement R1, Part 1.4 should provide an exclusion for CIP Exceptional Circumstances. (47) CIP-010-1, Requirement R2, Part 2.1, is an internal control in itself. There is no need to have the preamble in R2 of identifies, assesses and corrects deficiencies; all the requirement needs to have is the table. Does the SDT intend to have Responsible Entities have identify, assess and correct around how they identify, assess and correct changes or does the SDT want the Responsible Entity to verify the changes, not the controls? Internal controls are unnecessary in this instance because the requirement is seeking an activity that is results based. (48) CIP-010-1, Requirement R3, the timing for performing an active vulnerability assessment is confusing. Part 3.1 states 15 calendar months and Part 3.2 states at least once every 36 calendar months. We suggest keeping active vulnerability assessments to Part 3.2, or once every 36 calendar months. (49) CIP-011-1 Part1.1 and 1.2 – Please change "Methods" to "Method(s)" and "Procedures" to "Procedure(s)". This is a long-held standard that NERC has used to indicate when there might be one or more than one item. Otherwise, the Parts literally compel more than one method and procedure when one might be sufficient. (50) CIP-011-1 Part 1.3 – Part 1.3 was struck in this version and focused on the periodicity of assessing adherence to the BES Cyber Information protection program. On the one hand, it seems odd to strike this requirement when it appears to be one of the few requirements that actually focus on an internal control. On the other hand, it meets two of the criteria (i.e. administrative and periodic) identified in the Paragraph 81 project for retirement of requirements. Perhaps, NERC needs to document what they consider good periodic review for these types of requirements in another document on internal controls for the CIP standards so registered entities will know what standard they are being measure against. (51) CIP-011-1 Part 2.2 – Why is the second bullet regarding "actions taken to prevent unauthorized retrieval of BES Cyber System Information" not consistent with the first bullet of Part 2.1. It seems they should be consistent.

(1) We support the concept of internal controls and agree that finding a violation for each instance is burdensome and unreasonable and evaluating possible deficiencies is a more efficient use of resources. (2) However, located throughout v5 is this section: "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . . The term documented processes refers to a set of required instructions specific to the Responsible Entity and to achieve a specific outcome. This term does not imply any particular naming or approval structure beyond what is stated in the requirements." We find that this direction implies without making it clear that a set of internal controls (Internal Controls Environment) are required in order to be in compliance. Without an Internal Controls Environment, a registered entity cannot maintain a state of compliance with the requirement. We believe that this is an unreasonable burden for those small utilities who currently do not have a large internal audit function or internal controls based upon COSO. (3) In the Fall 2012 ERO Compliance Enforcement Authority Workshop, it clearly states that an entity's Internal Control Environment is to be audited based upon the COSO Framework and control types. The inclusion to identify the control activities as per the COSO components of internal control is not a requirement, however, the enforcement and auditing of the requirements will use COSO as the determining factor for completion and appraisal of compliance. Furthermore, if COSO is to be used as the

'industry standard' for auditing control activities, the above training and guidance does not clearly identify what are the definitions of the components and the level of control categories acceptable for compliance. More details, guidance and training are necessary to ensure that these COSO concepts are communicated to the registered entities in order to ensure that the registered entities meets the expected controls baseline for compliance. (4) Does the focus on the registered entity's Internal Controls Environment replace the previous Internal Compliance Program (ICP) directed by FERC and assessed using the CPAW audit template? If so, where is this documented and what are the requirements for an Internal Control Environment? Doesn't this new approach constitute a new set of indirect requirements to be placed on the registered entity that has not gone to a ballot vote by industry? If the COSO model is used and approved, are there some deficiencies that can be accepted by the registered entity as per their individual Risk Assessment? If not, then what is the requirement and guidance for an individual Risk Assessment for assessing risk to the reliability of the bulk power system? (5) As per COSO, the Internal Controls-Integrated Framework is based upon five components for a set of financial statements, not control systems. How does NERC believe that this set of audit components and internal controls relate to control systems and their IT cyber systems? (6) In the CIP-006-5 RSAW, it identifies these types of COSO Components: Control Environment (CE), Risk Assessment (RA), Control Activity (CA), Information and Communication (IC), and Monitoring (M) with these categories; Preventive, Detective, and Corrective. The inclusion to identify the COSO components and control categories of internal control is not a requirement; however, the enforcement and auditing of the requirements will use COSO as the determining factor for completion and appraisal of compliance. If COSO is to be used as the 'industry standard' for auditing control activities, the requirements and RSAW guidance do not clearly identify what are the definitions of the components and the level of control categories acceptable for compliance. (7) For a controls environment to be considered 'effective' or strong, the registered entity must implement layers of the previous mention categories: Administrative, Technical and Physical. The minimum for an effective control is to have at least one control activity in each of the three categories: preventative, detective and corrective. The strongest controls implement all nine layers (preventative, detective, and corrective implemented by using administrative methods, technical methods, and physical methods). We believe that this is an unreasonable burden for those small utilities who currently do not have a large internal audit function or set of controls based upon COSO. (8) In CIP-006-5 RSAW, it states: "Where the CEA is to report a possible non-compliance: 1. Deficiencies that create a high risk to the reliability of the bulk power system may be reported by the CEA as a finding of possible non-compliance. The CEA is to use his/her professional judgment to determine whether this is a necessary or appropriate action. NERC's Enforcement Team has publically stated that they are recommending that SMEs be removed from the regional audit staff and replaced with professionally certified and trained auditors; not staff with electric utility experience. How does a certified professional auditor understand the potential high risk to the reliability of the bulk power system and make that determination of possible non-compliance and how can that be consistently applied to all certified professional auditors? Is there a master list of what constitutes a potential high risk to the BES? One could decide either way that an unauthorized access to the PSP, an open port, or an improperly managed ACL list is a potential high risk to the BES. What is the threshold to a potential high risk of the bulk reliability of the BES? (9) In CIP-006-5, it states, "The CEA can expect the Responsible Entity to have maintained a list of the deficiencies it identified as presenting minimal risk to bulk electric system reliability and shall, in that list, indicate: • the date the Responsible Entity identified the deficiency and the nature of the deficiency, • how the Responsible Entity determined the risk of the deficiency, • the manner of correction, the name of the person that reviewed the completion of correction, and the date of the completion of correction." The CIP-006-5 RSAW states that the CEA can expect the Responsible Entity to have maintained a list of deficiencies. There are no requirements explicit for a list with the bullets points listed above? Is the list subjective and how long should this 'expected' but not required list be kept for record keeping? Is the list to be reviewed and signed by the designated NERC CIP Manager? (10) We are concerned about the consistent evaluation of internal controls from Regional audit staff. How is NERC planning to train the Regional auditors to ensure consistency during compliance audits? There are so many possible deficiencies that could occur on a daily basis and there is not clear guidance as how the Regions will decide on what is a possible high risk to the reliability of the bulk power system. (11) We recommend the SDT provide additional information in the RSAWs to show how the Regional auditors would assess compliance with a risk and control-based standard. With the change on focus for CIP version 5 in finding errors and fixing them, how are the Regions going to determine when a PV is to be issued? The Technical Justification and the RSAW do not provide enough information for the registered entity to determine when a CIP deficiency crosses the threshold of a possible high risk to the bulk power system. (12) We recommend adding more detail, perhaps including an application guidelines section for acceptable remediation of the deficient control. What documentation would then be required? The internal controls used to remedy deficiencies could turn into another documentation exercise instead of focusing on effective cyber security. We recommend the SDT consider ways of satisfying remediation without creating an unnecessary administrative burden for maintaining compliance. (13) The Measures in the standards do not appear to reflect the internal controls approach. When the requirements use the "identifies, assesses, and corrects deficiencies" language, should the measurement reflect this language that focuses on internal controls rather than the requirement? After all it is the internal control that is to be audited rather than the requirement directly. (14) Not all of the requirements use the "identifies, assesses, and corrects deficiencies" language? For those requirements that do not use this language, will compliance monitoring focus on individual instances of non-compliance? Will a zero-defect standard be used for these? (15) There are many requirements in the standards that look like internal controls. For example, there are several requirements that require a periodic activity or evaluation of the associated process or procedure. These requirements appear to be

internal controls. This causes confusion over what exactly NERC's view of internal control is and how they will be evaluated and monitored. As a result, we think better supporting documentation for what constitutes an internal control for CIP and how those internal controls will be monitored and evaluated by auditors should be developed. Furthermore, we think the SDT needs to consider eliminating many of these requirements that appear to be internal controls. (16) The standards inconsistently use "one or more processes" language. In some standards, this language was changed simply to "processes". In other standards, this language was introduced in place of "processes". CIP-008-5 Parts 1.1 and 1.2, CIP-005-5 Part 1.5, and CIP-011-1 Parts 1.1 and 1.2are examples of inconsistencies.

Individual

Jack Stamper

Clark Public Utilities

Group

NPCC

Guy Zito

We support these 10 Standards, the Implementation Plan and the set of Definitions but have the following comments For clarification, suggest adding "mimic display" to the second paragraph of CIP-007 R5 Rationale, resulting in "Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.)." CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not acceptable to the Canadians. Recommend new words that are acceptable to the Canadians. For consistency, recommend changing CIP-008 R2 Part 2.1 from "at least once every calendar year, not to exceed 15 months" to "at least once every 15 calendar months" For clarity, recommend changing CIP-009 R1 Part 1.5 from "One or more processes to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery." to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

Individual

Steve Alexanderson P.E.

Central Lincoln

This draft significantly changed CIP-002 R1 and the new language is very confusing. Central Lincoln understands that per R1 and R1.1, a responsible entity must implement a process to "Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset" using assets listed in bullets 1 through 6. When we try to parse the quoted statement above into more manageable bits, we see that the process must "identify each high impact BES Cyber System at each asset" Further parsing yields "identify at each asset." Our interpretation of this language calls for the process to require the physical marking of every asset that meets one or more of the criteria 1 through 6 while also meeting one or more of the criteria 1.1 through 1.4 of Attachment 1. This is a huge change from all prior versions of CIP-002. We don't believe the SDT intended for the process to require physical marking of relevant assets, but to require the listing of the relevant assets. We suggest "Identify and list each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at the asset level," and a similar rewrite of R1.2 would more closely match the SDT's intent.

Individual

Bernard Pelletier

HQ Transenergie

CIP-008-5 R.1.2 – Notify ES-ISAC may represent a national issue for Canadian entities. Recommends rewording to be sure the center to report to is approved by federal government like "… notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) or any other entity approved by their respective federal government

Individual

Daniel Inman

Minnkota Power Cooperative, INC.

Over Comment: We don't feel as though the current wording of the CIP Version 5 standards accomplishes the intended purpose. The stated purpose is "To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES." We believe that the standard as written evaluates only the impact of a degradation to a group of Facilities instead of evaluating the degradation of a BES Cyber System. Requirements R1.1 through R1.3 specify that the BES Cyber System is to be evaluated as a high, medium, or low impact as defined by Attachment 1. Attachment 1 gives criteria for evaluating the Facility or groups of Facilities, but not for BES Cyber Systems. The BES Cyber Systems

are globally given the same impact rating as the Facility or group of Facilities. We believe that once the Facility has an impact rating assigned, each individual BES Cyber System associated with the Facility should be evaluated for its impact on the Facility and given its own impact rating equal to or lower than the Facility's overall rating. This could be done by adding an Attachment 2 which describes the criteria for rating the impact of the BES Cyber System on the Facility. CIP-002-5 Guideline and Technical Basis: Requirement R1 on Page 22, last sentence of the first paragraph is confusing; "The criteria in Attachment 1 provide a measure of the impact that the BES assets that these BES Cyber Systems support, on the reliable operation of the BES." CIP-002-5 Attachment 1 criteria 2.1: The description uses "single plant location" and "single Interconnection" in the same sentence. In some situation these items may not have the same meeting. For example, two generating units in the same plant may connect to two different substations, or two different plants could connect to the same substation. Additionally, would you add multiple generators with different interconnection facilities which connect to different parts of the same substation? Need clarification on this criterion. CIP-002-5 Attachment 1 criteria 2.3: Is the term "generation Facility" in this criterion designed to cover a single unit at a facility, or all units at a single plant or Interconnection, as described in section 2.1? CIP-002-5 Attachment 1 criteria 2.3: The guidance document makes it sound like the Planning Coordinator would make the determination whether a plant is critical, not the Transmission Planner. The guidance document should be revised to reflect the standard, which states "Planning Coordinator or Transmission Planner", implying either Entity can make the determination. CIP-002-5 Attachment 1 criteria 2.3: Is the phrase, "such as due to a Category C3 contingency" intended to provide guidance to what faults to run? Is the term "Adverse Reliability Impact" which is used in Attachment 1, meant to be the criteria for all types of contingencies? CIP-002-5 Attachment 1 criteria 2.5: We would like to see clarification on how the following items are handles: 1) is/how is a DC line counted? 2) If you have a tie between two subs that has a transformer in series, does the line receive a weighting factor (seems to per guidance)? Do you use the higher or lower voltage? Is it the same for both ends of the line? Some notes are added in guidance, but they are not sufficient. CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, it was clarified that radial facilities that only provide support for "single generation facilities" would not be included. What is the definition of a "single generation facility"? Uncertain situations might include two base load turbines aggregated on one line or wind farm collector subs which have multiple sites feeding into a single high voltage collector sub? CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, in the last bullet on page 27, it is not clear what the statement "In these cases" is referring to, whether the designation as a single facility or multiple facilities. CIP-002-5 Attachment 1 criteria 2.5: From the guidance document, in the last bullet on page 28. How would classification of the number of substation connections be handled if two lines are parallel between the same two subs, but one has been tapped for local, non-networked load service? CIP-002-5 Attachment 1 criteria 2.8: Based on my reading of the standard, it appears that the loss of a Transmission Facility must result in loss of ALL of the generation that comprises the generation Facilities. For example, consider two 1000 MW generators located in a single plant and therefore given a Medium Impact Rating based solely on criterion 2.1. We believe that degradation of a Transmission Facility which only resulted in the loss of one of the two units would not meet the criteria in 2.8 (unless that generator was deemed critical on its own merits as well). We would like to see emphasis added that degradation of the Transmission Facility must result in loss of ALL of the generation that was included to force a Medium Impact Rating. CIP-002-5 Attachment 1 criteria 2.9: What is an automated switching system? Can this be more specifically defined, maybe by adding it to the guidance document? We believe this term should only be included if it is given a specific definition. Also, would end-to-end tripping be included in this definition? CIP-002-5 Attachment 1 criteria 2.9: We believe the following section in the guidance document is a run-on sentence and needs revision: "Special Protection Systems and Remedial Action Schemes may be implemented to prevent disturbances that would result in exceeding IROLs if they do not provide the function required at the time it is required or if it operates outside of the parameters it was designed for Generation Owners and Generator Operators which own BES Cyber Systems for such Systems and schemes designate them as medium impact." We suggest inserting a period before the words "Generation Owners" if this accurately captures the intent of the SDT in drafting the language. CIP-002-5 Attachment 1 criteria 2.10: The guidance document specifies that the SDT "chose the term 'Each' to represent that the criterion applied to a discrete System or Facility". Our interpretation of this statement is that a regional UFLS program which sheds more than 300 MW and is comprised of multiple independent UFLS relays in at different substations would not be given a Medium Impact Rating at the NERC or RRO program level. An individual relay would only be given a Medium Impact Rating if that relay shed more than 300 MW by itself. Is this understanding correct? CIP-002-5 Attachment 1 criteria 2.10: The guidance document notes that the ERCOT LaaR demand response program is excluded from the 2.10 criterion. Does any load management program used to off-set resources qualify for exclusion from this criterion? If so, please include a generic statement to that effect in the guidance.

Individual

Mike Marshall

Idaho Power Company

There is general agreement with the movement of the standards away from zero tolerance to an "identify and correct" philosophy so long as checks and balances are in place and the regulator supports the apparent spirit of what the Standards Drafting Team seems to have intended. Next, Criteria 2.8 of Attachment of CIP-002-5 implies that a transmission facility providing interconnection to a generation facility is considered to be in the medium

impact category if the generation owner categorized the generation facility as medium impact. In the case where the generation is not owned by the Transmission Owner this could put the Transmission Owner at the mercy of the Generation Owners application of the standard even if the Transmission Owners facilities would not otherwise be in scope. Next, the Standards continue to exempt cyber assets associated with communications networks and data communication links between Electronic Security Perimeters. Therefore, the internet protocol network used to monitor, control, and provision communications network infrastructure owned by electric utilities are exempted. Exempting the utility owned communications infrastructure creates a cyber security issue. Next, CIP-004-5 R5.2. requires that access for employees that are reassigned or transferred be change within 24 hours. The time frame listed is difficult to comply and is unnecessarily short when the employee is remaining with the company if the transfer or reassignment was in the normal course of business and not for disciplinary reasons. Next, in CIP-006-5 R1.1. the change description in the table states that Physical Access Control System (PACS) do not need to be in a Physical Security Perimeter (PSP). Does that include everything related to PACS? This wording seems contrary to the requirement wording of CIP-006-5 R1.7 in which physical access controls are required. Further clarification is needed. Next, the CIP-007-5 R2.2. change from 30 days to 35 days is excellent. This allows utilities to manage patches monthly coinciding with vendor releases without running into issues of the requirement being less than a full month. Practically however there is no reason this shouldn't be extended to 40 days to accommodate time to review the vendor releases. However, the additional 5 days will ensure that those utilities with patch management programs are not penalized due to variations in patch release dates from month to month. Next, the CIP-010-1 R3.3. requirement seems redundant with CIP-010-1 R1.5. The entity is required to test the new device against its baseline and cyber security controls for adverse affects (under R1.5.) and then again is required to do a vulnerability assessment which again is a check (under R3.3.) against cyber security controls. This needs further clarification as to what the difference for new cyber assets under these two sub-requirements. Next, the definition of a Cyber Asset should not include the nondescript term "data" as the majority of data in the cyber asset is not related to the security of the device. This could potentially be construed as all data; including data unrelated to CIP, the device, or security and could pose great logistical challenges. Clarification of "data" or removal of the term needs to be addressed. Next, the definition of an Electronic Access Control or Monitoring Systems ("EACMS") should explicitly exclude tools for vulnerability assessments and other monitoring not associated with real-time "access" monitoring. The current wording seems to include all devices that perform monitoring functions even if they are not associated with real-time "access" monitoring. In addition, CIP-004-5 R4.2. Requires a quarterly authorization records review. It seems that this is a step backward in security and is simply a documentation check. Documentary evidence is inherent the in the standards and a documentation check does not provide additional security. Also, the CIP-007-5 R4.1.2. requirement calls out failed access attempts and failed login attempts. It is unclear as to why "failed access attempts" and "failed login attempts" are separated. Are "failed access attempts" referring to physical access attempts? Are they referring to some other form of electronic access to undermine the login process? Further clarification is needed.

Group

Snohomish County PUD

Benajmin Beberness

CIP-002-5 Comments: Snohomish County Public Utility No. 1 ("SNPD") does not support CIP-002-5 – Attachment 1, Section 2.12. SNPD does not believe that all Transmission Operator control centers not included in the High Impact Rating should be automatically included in the Median Impact Rating. SNPD understands that control centers require an appropriate level of protection for the bulk electric system and its identified components. However, SNPD urges the Standard Drafting Team (SDT) to establish appropriate levels of impact (High, Medium & Low) through the application of a 1500 MW generation and 1000 MVAr bright-line thresholds. The SDT has made reasonable changes to the treatment of small BA and GOP control centers. Corresponding changes should be made to the treatment of small TOPs. SNPD supports the American Public Power Association's ("APPA") comments and proposals for CIP-002-5 and intends to ballot negative on CIP-002-5. However, if the APPA proposal is adopted, SNPD intends to change its ballot from negative to affirmative in the recirculation ballot. CIP-005-5 comments The requirements contained within NERC CIP v5 (current draft) need to be tempered with a risk-based approach as documented in NIST SP 800-37, Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" or DOE/OE-0003, "ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS," May 2012. CIP-009-5 comments 1.5 The requirement to preserve a corrupted drive or a mirror of a failed system before proceeding with recovery is not practical. A failed system is a failed system. The complexities of a system in a data center or enterprise environment may severely limit our capabilities to preserve a system in its failed state.

SNPD would like to begin with a general comment on the Critical Infrastructure Protection ("CIP") Version 5 and CIP-010 and 011 Cyber Security Standards. The purpose given for CIP-002 reads in part: "To identify and categorize the BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES". Yet this same standard mandates a Medium Impact Rating in its Impact Rating Criteria to "Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H) above" (per Attachment 1, Section 2.12). This implies that every energy control center or backup control center used to perform the obligations of a Transmission Operator is inherently necessary for the reliable operation of the BES which is not

factually correct. SNPD Control center operates a Local Network that provides a distribution function to its customers. SNPD does not control frequency, voltage schedules, or calculate Available Transfer Capability ("ATC") on a WECC rated path. The only operating functions SNPD can perform to support BES reliability is to provide data and drop load if requested by the Bonneville Power Administration (SNPD's BA and TSP). However BPA has the ability to independently island or isolate the SNPD system. Furthermore, the definition of a BES Cyber Asset definition in these Draft Standards is "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System.". SNPD is a distribution utility that also meets the registration criteria of a Transmission Operator and does have a Control Center. However, as a Distribution utility with very small generation resources, there is nothing that the loss, compromise or misuse of its cyber systems or cyber assets could have on the reliable operation of the Bulk Electric System. The Operations Center is in place to address planned and unplanned outages and load restoration on a Local Network. The goal and main mission of the SNPD Operations Center is to ensure that customer service levels are met and safety procedures are followed. The draft criteria for Attachment 1, Section 2.12 creates an unnecessary and onerous burden to utilities such as the SNPD without providing any benefit to the reliability of the Bulk Electric System. The draft criteria for Attachment 1, Section 2.12 should be amended so that it is clear that it applies only to those entities whose operations could have an impact on the Bulk Electric System. This can be accomplished by implementing one of the APPA recommendations.
Individual
Jennifer White
Alliant Energy
Alliant Energy acknowledges the substantial work done by the Standards Drafting Team to solve the industry issues between drafts 2 and 3, and we support most of the changes. Those changes allowed an affirmative vote on all ballots. We do have additional comments, however, that we would like to submit for consideration: Alliant Energy disagrees with the removal of "annual" obligations from all the Standards. The "once every 15 month" language can lead to a perception of loosened rigor around these activities, as it will allow entities to omit the activity for a calendar year. This decreases reliability and deviates from other NERC Standards. We recommend use of the term "annual," allowing the entity to define that term within its program, or, the alternative "Once per calendar year, not to exceed 15 calendar months." CIP-003-5 R4 – This requirement should not include the "identify, assess, and correct" language, as it is a results-based requirement where deficiencies are unlikely and, if they do exist, create a lot of risk for the organization related to unauthorized signatures. Also, strike the last sentence related to a change in the delegator. If either the delegator or the delegate changes, the delegations should be reviewed/updated. CIP-010-5 R1.4 – The "guesswork" initiated by CIP-010-5 R1.4.1 does not add value. This is especially true if the only thing that must be tested by R1.4.2 is the list of controls identified with the guesswork. The entity is enticed to round down. Recommend striking 1.4.1 completely and change 1.4.2 to say "Following the change, verify that cyber security controls are not adversely affected." Keep 1.4.3. CIP-010-5 R1.5 – We do not feel that emergency change controls necessary for reliability should be a TFE if related to a CIP Exceptional Circumstance. Recommend adding that verbiage to the beginning of the requirement. Alternatively, if it is the intention of the drafting team to indicate that a TFE is necessary if an entity doesn't have a test environment for a High Impact BES Cyber System, the TFE language should be moved down into the 1.5.1 or 1.5.2 to eliminate references to a TFE for each change.
As to the Implementation Plan - the verbiage allowing ambiguity until March 31, 2014 related to Version 4 is unreasonable. The deadline for FERC approval should be moved 6 months ahead of that deadline to allow entities who have to make transitions to Version 4 to hold off on infrastructure purchases until absolutely necessary without the risk that those purchases will be made moot and wasteful should FERC approve V5 (skipping V4) in the 11th hour. Set a reasonable deadline for skipping V4.
Individual
Jim Cyrulewski
JDRJC Associates, LLC
Individual
Melissa Kurtz
US Army Corps of Engineers
Individual
Alice Ireland
Xcel Energy
1) CIP-004-5 Requirement 4.1.3 expands the scope of personnel beyond CIP and requires a need to restrict and monitor access to additional data centers for individuals with "potential" physical access to systems containing CIP Information. For CIP Information, the risk impact is low as physical damage to equipment containing electronic information doesn't have any direct impact to the operations and reliability of the BES. In the General Summary of Consideration of Comments, the SDT defines physical access as both access to hard copy data and access to

equipment used for storing electronic copies. Based off the Applicable systems definition in CIP-006-5 there is no requirement to physically protect access to electronic systems that store information so to call in physical access controls for these devices under CIP-004-5 generically, is beyond the scope of the standard. 2) For consistency, we recommend modification to CIP-004-5 R5.3 language to follow the wording in R5.1 as it relates to the timeline to remove access. 3) CIP-005 R2.1 is still unclear if a VPN is an acceptable form of remote access. 4) CIP-007 R5.6 "where technically feasible" should be removed. 5) Suggested clarification to CIP-002-5 d3, Attach. 1, 2.1: "…For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, if lost or compromised, within 15 minutes, adversely impact the reliable operation. 6) In the Guidelines and Technical Basis section for CIP-006-5 under Requirement 1, Methods to monitor physical access include: "…These alarms must provide for immediate notification to personnel responsible for response." We would suggest this section be edited to match the requirements of CIP-006-5 R1.5 and R1.7, "within 15 minutes of unauthorized physical access. It would also be suggested that the wording about Outage records be removed from the Guidelines and Technical Basis section as the Requirement was removed.

Individual

Jonathan Appelbaum

The united illuminating Company

UI seeks clarity on several topics in the Standard to allow implementation to progress correctly. Definitions- Is an EAP a PCA?; Bes Cyber System definition uses the word logically that may be mistakenly interpreted to mean networked instead of validly grouped; Implementation – Please maintain flexibility for an entity to either move from V4 to V5 or straight to V5. CIP-005- Can a switch be divided into multiple ESPs or have one port outside the ESP provided no routing between VLANs? And For R1.5 does two distinct machines need to be utilized, one as a firewall, and one as Intrusion prevention or can it be on one device (order706A par:66) and when the EAP is segmented into multiple networks where one is LAN is critical and one is Non-critical does an IDS need to be on each network segment monitoring inbound/outbound traffic on the segment or just at the EAP monitoring inbound/outbound traffic? CIP-007 R4.4 – A manual log review is a labor intensive outdated approach. The technical guidance should allow for use of network behavior analysis or other automated review process for this requirement. CIP-008 and CIP-009 both have document update requirements which are administrative which should be considered for removal. CIP-009 in technical guidance states recovery plans are BES Cyber Information which is not true by Definition and CIP-011.

Individual

Maggy Powell

Exelon Corporation and its affiliates

Exelon appreciates the hard work and devotion of the CSO 706 drafting team. The improvements made to draft 2 represent significant progress. Thank you for your effort. Below are remaining questions and comments that we request the SDT give serious consideration for revision to the proposed suite of CIP V5 standards: GENERAL: • Internal Control Language and VRFs/VSLs– The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a dramatic change in approach taken very late in the development process of the CIP V5 standards. Exelon appreciates the SDT's attempt to recognize that certain requirements should not focus on individual instances of failure as a sole basis for violating the standard and that enabling corrective action over compliance burden is preferable to the pursuit of reliability. However, the newness of putting this concept into the standard language raises significant uncertainty and confusion. Unfortunately, the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach (nor does it indicate what is not considered a violation). At the core of the confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, Exelon is taking a leap of faith that NERC leadership and staff will work diligently and collaboratively to clarify the compliance component of this language to ensure that it fulfills the supported intent and creates no added compliance burden. Exelon supports the concept, but much more work is needed to understand and support the compliance obligations and enforcement measures around the concept. • Previous versions of the CIP standards incorporated headers to group the requirements. This practice was particularly useful to internal compliance management programs that deploy data mining, report creation/generation or database building by creating a consistent framework to the standards. Please consider returning to the practice by adding the following headers to the CIP V5 standards: • CIP002-5 Cyber Asset and Cyber System Categorization • R1. Identification and Categorization • R2. Review and Approval • CIP003-5 Security Management Controls • R1. Review and Approval of BES Cyber Systems Policies • R2. BES Cyber Systems Policies • R3. Identification of Leadership • R4. Delegation of Authority • CIP-004-5 Personnel and Training • R1. Security Awareness Program • R2. Training Programs • R3. Personnel Risk Assessments • R4. Access Management • R5. Access Revocation • CIP-005-5 Electronic Security Perimeter • R1. Electronic Security Perimeter • R2. Interactive Remote Access • CIP-006-5 Physical Security of BES Cyber Systems • R1. Physical Security Plans • R2. Visitor Control Programs • R3. Maintenance and Testing of Physical Access Control Systems • CIP-007-5 Systems Security Management • R1. Ports and Services. • R2. Patch Management • R3. Malicious Code Prevention • R4. Event Monitoring • R5. System Access Controls • CIP-008-5 Incident Reporting and Response Planning • R1. CSIRP Specifications • R2. CSIRP

Implementation and Planning • R3. CSIRP Review, Update and Communication • CIP-009-5 Recovery Plans for BES Cyber Systems • R1. Recovery Plan Specifications • R2. Recovery Plan Implementation and Testing • R3. Recovery Plan Review, Update and Communication • CIP-010-1 Configuration Change Management and Vulnerability Assessment • R1. Configuration Change Management • R2. Configuration Monitoring • R3. Vulnerability Assessments (Move to CIP-007-5. Please see comment below) • CIP-011-1 Information Protection • R1. Information Protection • R2. BES Cyber Asset Reuse and Disposal (Move to CIP-010-5, R4. Please see comment below) • Guidelines and Technical Basis, all V5 standards – At first glance, beginning the Guidelines and Technical Basis with "Section 4" seems to be citing section 4 of the Guidelines portion. Consider revising the title to read: "Scope of Section 4 Applicability of the CIP Cyber Security Standards. The same revision should be made to the other CIP V5 standards that incorporate the same section. • Guidelines and Technical Basis, all V5 standards (Reminder) – For continuity and to avoid future confusion, please revise guidance to be consistent with any changes made to the standard language. • Implementation Plan (Reminder) – As with the Guidelines and Technical Basis, please confirm that the implementation plan language is consistent with any changes made to the standard language. DEFINITIONS: • BES Cyber Asset – Please consider adding acronyms as in other definitions to read ("BES CA"). • BES Cyber System – Please consider adding acronyms as in other definitions to read ("BES CS"). • BES Cyber System Information – Please consider adding acronyms as in other definitions to read ("BES CSI"). • Control Center – As previously requested, please consider revision of the Control Center definition to read "CIP Control Center." A number of other standards refer to "control center" and the term as defined in the CIP V5 proposal is inappropriate to other situations. Identifying the definition as a CIP Control Center will help prevent confusion and inappropriate application of this definition to other standards. If the drafting team is unable to revise the definition title, please clarify that this definition is not applicable to other standards that utilize reference to "control center" in the lower case. CIP-002-5: • Background – On page 9 of CIP-002-5 clean version, Remove the "Card system" reference cited for PACS since that could be confused with card readers which are excluded as locally mounted hardware or devices the definition. Further distinction may be needed. • Attachment 1 – Attachment 1, 3. Low Impact Rating - For clarity, please change the word "Section" to "Criteria" to read: "BES Cyber Systems not included in Criteria 1 or 2 above…" This is more consistent with the title of Attachment 1 as Impact Rating Criteria and avoids confusion to reference of other sections of the standard. • Attachment 1 – Attachment 1, 3. Low Impact Rating – The addition of the sub-criteria (3.1 through 3.6) is a duplicate of what is already specified in Requirement 1 and does not necessarily clarify the language. CIP-003-5: • CIP-003-5 R1.1-R1.9 (Reminder) – For continuity and to avoid future confusion, please make sure that all titles referenced in the sub-requirements are consistent with final titles in the standards and track with any changes made though the development process. • CIP-003-5, R2 – The necessity of R2.4 is not clear. More guidance is needed for low assets to determine when something is considered a Cyber Security Incident since we are not required to monitor the electronic or physical perimeters for Low Impact systems. Is this to be defined by policy or by some other means? CIP-004-5: • CIP-004-5, R5.2 – As previously noted, the treatment of transfers (employees in good standing) remains more severe than for terminations in that terminations allow 30 days to remove all access. As well, the proposed CIP-004-5 requires that entities are to remove access by the end of the next calendar day following the determination that access is no longer needed. This is a new date that would require new administrative tracking. CIP-005-5: • Guidelines and Technical Basis – The first bullet under paragraph 2 in the Requirement R1 discussion cites 'Associated Protected Cyber Assets.' Associated should be lower case as it is not part of the definition. Same correction needed in the 4th paragraph starting "For example," of the same R1 section. CIP-007-5: • CIP-007-5, R2.2 - The rationale states a 30-day time frame while the requirement states 35 days. Please revise the rationale to be consistent with the requirement language. CIP-008-5: • CIP-008-5, R1.2 – The intent of the language in R1.2 appears to be to align the hour time frame as triggered by the determination rather than identification; however, the language can more clearly express that intent. Please consider the following revision: One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and to notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), which may be only a preliminary notice, shall not exceed one hour from determination. CIP-008-5, R3 – This requirement should include the internal controls language and allow entities to implement, in a manner that identifies, assesses, and corrects deficiencies since the time needed to complete a review, process updates and notifications is really contingent upon the severity and type of event. The 90 calendar days is an administrative requirement lending itself to a programmatic, internal control. CIP-009-5: • CIP-009-5, R1 Tables – R1.5 can be worded more clearly to align the device capability with preserving data. Please consider the following revision: "One or more processes to preserve data (per device capability) for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan. Data preservation should not impede or restrict recovery." • CIP-009-5, R1 Tables – M1.5 should be revised to match: "An example of evidence may include, but is not limited to, procedures to preserve data where the device is capable, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery." CIP-010-1: • CIP-010 R3 – This requirement addresses Vulnerability Assessments, which may more appropriately align with CIP-007 as the standard geared to mitigating vulnerabilities. Please consider relocating CIP-010 R3 to CIP-007 as either R1 or as R6. CIP-011-1: • CIP-011-5 R2 — R2 discusses BES Cyber Asset Reuse and Disposal. This activity often falls under Configuration Management. Please consider moving this requirement to CIP-010-5, R4.

Group

Lakeland Electric

Mace Hunter

Individual

Tom Bowe

PJM Interconnection, L.L.C.

Definitions--Interactive Remote Access-- has requirement within the definition. This requirement should be pulled from the definition and added to the requirement in CIP-005 R2.2. CIP-004 R3 In some situations employee history is not available/released (e.g. country of origin denies access to documentation or limitations with Juvenile record access) How to comply in such situations? CIP-005—R3.2.1 Define "applicable asset". "Applicable Cyber Asset" should be called "Applicable System" to align with wording in column "Applicable Systems". CIP-007—R1. (Rational). New term "Control Center Environment" was introduced. Could potentially have different meaning than Control Center. Clarification is requested. CIP-010—R1.1 Clear understanding could not be established on the wording "intentionally install". Clarification is requested. CIP-010 R1.4 When testing Cyber Security Access controls, CIP-005 focuses on changes to ESP access points and CIP-010 focuses on logical perimeter (excluding access points). How will configuration changes within CIP-010 impact cyber security controls within CIP-005? CIP-10 R1.5. For further understanding of the sentence "Where Technically Feasible" please provide an example of the circumstances where TFE could be filled.

Individual

Michael Moltane

ITC

ITC will be voting "Affirmative" on the CIP v5 ballots, but does have one concern we would like noted: The intent of the Critical Infrastructure standard seeks to establish an industry wide objective to identify the facilities and cyber system that is misused or rendered unavailable will adversely impact the reliable operation of the BES. The BES Cyber System Categorization currently presented under CIP V5 is undermined when excluding, by classifying as low impact rating, systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration. These facilities play a major role on BES operation and are receiving exclusion from protection and security controls very well defined and in line with FERC's Order 706. This exclusion does not foster the best outcome and leaves a major security hole and risk. The technical basis and guidelines presented for CIP-002-5 are very well connected to other NERC Reliability standards and provide a very good bridge to assure clear and consistent identification of systems and facilities.

Group

Florida Power & Light

Mike O'Neil

The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC's Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language ("in a manner that identifies, assesses, and corrects deficiencies" (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard's requirements. The proposed RSAW language regarding "deficiencies" and "self-reporting" does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase "in a manner that," which is itself prefaced by the words "shall implement," the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to

strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.

NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.

Individual

David Rivera

New York Power Authority

Individual

Greg LeGrave

Wisconsin Public Service Corporation

Concern regarding Implementation Plan: WPS is seeking clarification regarding the NERC Implementation Plan and how 2015 audits will be conducted with regards to Version 3 and Version 5 of these standards. It is important that registered entities understand these details during this year of significant transition.

Individual

Kirit Shah

Ameren

None

(1)Replace undefined term "adversely impact" with "Adverse Reliability Impact" throughout the standard and definitions document to be consistent with the defined term in the NERC Glossary. (2)The "within 15 minute time frame" included in the definition of BES Cyber Assets is problematic to provide evidence during the audit. Add some examples, in the Guidance Document, of BES Cyber Assets that would create an Adverse Reliability Impact within 15 minutes. (3)The time frames to revoke access are still problematic considering the risk to the BPS. For a transfer, when an employee is still in a good standing and is still employed, why must an access be removed by the end of the next calendar day? Keep it at 7 days. (4)Provide guidance on how to comply with CIP-007 requirements on Medium BES Cyber Systems serial connected devices; (patching, anti-virus, etc. on large number of programmable protective relays); why other measures implemented for substation assets, such as, physical protection, are not adequate? (5)Include example diagrams, in CIP-002, page 27, to provide guidance application of each bullet in criterion 2.5. (6)Flowchart in CIP-002, page 32, is confusing and may belong with other CIP standards.

Individual

Michelle D'Antuono

Occidental Energy Ventures Corp.

Occidental Energy Ventures Corp. (OEVC) would like to point out that CIP-002-5, Attachment 1, Item 1.4, would require that a 1500 MW GOP Control Center take on a High impact rating, while the rest of the Facility is Medium impact. Even if the criterion is intended to apply to multiple locations, we believe that the aggregated generation should be 3000 MW or greater – consistent with the risk level assigned to a BA Control Center.

OEVC is greatly supportive of the RSAWs being developed concurrently with the CIP standards. However, we would like to see all ten RSAWs – as the enforcement of the risk-based language introduced in many of the Draft 3 requirements is critical to our acceptance. In particular, we are concerned that if CEAs simply continue to evaluate compliance using historical auditing techniques, the impact to our resources (and theirs) will not change. Unfortunately, the posted RSAW for CIP-006-5 only reinforces our belief that a "business-as-usual" approach has been taken. OEVC saw nothing in the RSAWs indicating a sensitivity to cost/benefit or that some risk is to be expected. In fact, we mostly see a rehash of the language in the standard itself, which is not helpful. A specific item that we believe deserves far more consideration is CIP-003-5, R2. In our view, there is too much leeway for CEAs to interpret the associated measure for the four cyber policies that all Responsible Entities must implement. It only points out the types of documents or other records that serve as proof of compliance. (No RSAW has been provided, but if it follows the pattern of the one posted for CIP-006-5, it will have the same issue.) OEVC believes that in order to eliminate any ambiguity which will serve to incentivize the development of CANs or other interpretive enforcement documents at a later date, guidance must be provided on the expectations for evidence of implementation "in a manner that identifies, assesses, and corrects deficiencies, calls for processes to be continually monitored, gaps identified, and deficiencies corrected." The "Guidelines and Technical Basis" section of CIP-003-5 has some good examples of acceptable policy CONTENT – and which could be easily incorporated in the measures and the RSAWs.

Group

PNGC Group Comments

Ron Sporseen

Group

Dominion

Greg Dodson

Certain 'periodic' requirements identified within draft 3 don't include the "zero-defect" language nor relief under CIP Exceptional Circumstances. While a Registered Entity is expected to comply with CIP requirements if at all possible during a CIP Exceptional Circumstance, we do not believe Registered Entities should be burdened with self-reports associated with identified instances of non-compliance caused directly by a CIP Exceptional Circumstance. Although the timing of the execution of 'periodic' requirements can be scheduled, the timing of CIP Exceptional Circumstances is inherently unknown and can conceivably overlap the timing of scheduled periodic requirements in such a way as to put a Registered Entity out of compliance with those requirements. We believe it's in the best interest of the reliability of the BES to record and track these instances of non-compliance as part of the process of bringing the affected BES Assets back into compliance rather than through a self-report process. Definitions (Suggested language changes for clarity): - Cyber Assets FROM: Programmable electronic devices including the hardware, software, and data in those devices. TO: Entity programmable electronic devices. RATIONAL: Simplicity. There's no need to include hardware, software, and data as this is understood and redundant. - Cyber Security Incident FROM: A malicious act or suspicious event that: - Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, - Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System. TO: A malicious act or suspicious event that: - Compromises the Electronic Security Perimeter or Physical Security Perimeter or, - Disrupts the operation of a BES Cyber System. RATIONAL: The current definition is too broad and could be construed to require a review of single instances of erroneous network traffic (such as a mistyped URL). - Electronic Access Control or Monitoring Systems ("EACMs") FROM: Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Devices. TO: Cyber Assets that perform electronic access control or electronic access monitoring of Electronic Access Points. This includes Intermediate Devices. RATIONAL: The language in the definition is unnecessarily broad and pulls in devices other than those that are electronic access points into the ESP. - Physical Security Perimeter ("PSP") FROM: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control Systems reside, and for which access is controlled. TO: The physical border surrounding locations in which BES Cyber Assets, BES Cyber Systems, or Electronic Access Control or Monitoring Systems reside, and for which access is controlled. RATIONAL: Conforming language to use EACMs CIP-002-5 R1.1 and R1.2: For clarity, change the language of requirements R1.1 and R1.2 to correlate the asset being referred to in the sentence as one of the 6 asset classes identified in the main part of the requirement. The suggested language is "R1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, which are located at each asset in the list above; R1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, which are located at each asset in the list above; and" CIP-003-5: A clarification should be added to the Guidelines and Technical Basis section of CIP-003-5 for R1 to ensure Registered Entities and Compliance

Enforcement Agencies understand that a policy to demonstrate compliance with CIP-003 R1 isn't necessary if the Registered Entity doesn't have high impact and medium impact BES Cyber Systems. This clarification is needed to provide guidance to Registered Entities for determining when policies are and aren't needed. CIP-004-5: Given the lower Violation Risk Factor, R1 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 1.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may miss performing quarterly security awareness reinforcement. The language of R1 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented processes that collectively include each of the applicable items in CIP-004-5 Table R1 – Security Awareness Program." CIP-005-5: For clarity, part 2.2 should allow encryption to terminate at a firewall that protects an intermediate device in addition to the intermediate device itself. Part 2.2 should be rewritten to state "For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate Device or the firewall protecting the Intermediate Device." CIP-006-5: - Parts 1.5 and 1.7 include the term "BES Cyber Security Incident Response Plan" which is not a NERC defined term. Additionally, Parts 1.5 and 1.7 as written will have an unintended consequence of requiring Registered Entities to over-respond to instances of detected unauthorized access. The Parts incorrectly assume a one-to-one relationship such that events of detected unauthorized access on a physical security plan must also be investigated under the cyber incident response plan. Within the context of a physical security plan, a cyber incident response is triggered by the subset of detected events of unauthorized access that, upon the initial investigation phase of the physical security team, identify the possibility of a cyber breach. Cyber incident response teams are not typically contacted regarding all events of detected unauthorized physical security breaches and are dependent upon the physical security team to investigate and evaluate the circumstances behind the alarm. The requirement to notify the members identified on the cyber incident response plan of all alarms associated with "detected unauthorized access" prior to investigation by the physical security team is unnecessary and overly burdensome. The language of Part 1.5 should be changed to, "Issue an alarm or alert in response to detected unauthorized access through a physical access point into a Physical Security Perimeter to the personnel identified in the physical security plan within 15 minutes of detection." The language of Part 1.7 should be changed 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 physical security plan within 15 minutes of detection." The change recommended for Part 1.7 makes it consistent with Part 1.5 and in that an alarm or alert can only be generated based on a known detected event. - Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 3.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss the testing of locally mounted hardware or devices associated with a Physical Security Perimeter affected by the CIP Exceptional Circumstance on the 24 month cycle in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented Physical Access Control System maintenance and testing programs that collectively include each of the applicable items in CIP-006-5 Table R3 – Maintenance and Testing Program." CIP-007-5: The TFE language of Part R5.6 is unnecessary given the ability to use either technical or procedural controls for enforcement. Additionally, the "per Cyber Asset capability" language used in Part 5.4 should be incorporated into Part 5.6 for consistency. The language of Part 5.6 should be clarified as follows "For password-only authentication for interactive user access, technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months." CIP-008-5: - Given the lower Violation Risk Factor, R2 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Part 2.1 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss the testing of a Cyber Security Incident Response Plan on the 15 month cycle in deference to activities that restore the normal operation of the Bulk Electric System. The language of R2 should be changed to, "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, each of its documented Cyber Security Incident response plans to collectively include each of the applicable requirement parts in CIP-008-5 Table R2 – Cyber Security Incident Response Plan Implementation and Testing." - Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Parts 3.1 and 3.2 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of when a periodic activity is due, a Registered Entity may appropriately miss 1) updating a Cyber Security Incident Response Plan within 90 calendar days of testing the plan (or an actual incident) or 2) updating the Cyber Security Incident Response Plan within 60 calendar days of identifying changes that may be required to execute the plan in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, "Each Responsible Entity shall maintain, in a manner that identifies, assesses, and corrects deficiencies, each of its Cyber Security Incident response plans according to each of the applicable items in CIP-008-5 Table R3 – Cyber Security Incident Response Plan Review, Update, and Communication." CIP-009-5: Given the lower Violation Risk Factor, R3 should include the "zero-defect" language to eliminate the possibility of a Registered Entity having to self-report under Parts 3.1 and 3.2 as a result of a declared CIP Exceptional Circumstance. It's conceivable that a Registered Entity that has a major disruption coincident with the timing of

when a periodic activity is due, a Registered Entity may appropriately miss 1) updating a recovery plan within 90 calendar days of testing the plan (or an actual recovery) or 2) updating the recovery plan within 60 calendar days of identifying changes that may be required to execute the plan in deference to activities that restore the normal operation of the Bulk Electric System. The language of R3 should be changed to, "Each Responsible Entity shall maintain, in a manner that identifies, assesses, and corrects deficiencies, each of its recovery plans in accordance with each of the applicable items in CIP-009-5 Table R3 – Recovery Plan Review, Update and Communication." CIP-010-5: No Comments CIP-011-5: No Comments

Individual

Nathan Mitchell

American Public Power Association

APPA does not believe that the SDT's response to comments fully addressed the substantive concerns we raised in comments on the prior draft with respect to the applicability of CIP-002-5 to the control centers of Transmission Operators. Numerous public power and cooperative owned utilities pointed out in comments to CIP V5 draft 2 standards, that the TOP Control Center Applicability thresholds needed to be addressed in draft 3. Small responsible entities with control centers that do not control significant BES facilities should be subject to the low impact tier of the CIP Version 5 Reliability Standards. The Standard Drafting Team (SDT) has made reasonable changes to the treatment of small BA and GOP control centers. Corresponding changes should be made to the applicability to small TOPs. APPA provided the following comments on the draft 2 standards: APPA believes that Criterion 2.11 in Attachment 1 should at a minimum designate control centers with control of less than 300 MW of resources as Low Impact. This will clearly define a lower threshold as requested for in 2.10 above and reduce the burden of compliance for small entities. The BA and GOP medium impact thresholds were changed to 1500 MW, but the CIP Standard Drafting Team (SDT) was not able to come to consensus on a threshold that would properly differentiate between Medium and Low Impact for TOP Control Centers. APPA still believes that small TOP Control Centers that control Low Impact Transmission Facilities should not be included in the Medium Impact category. APPA offers the following recommended modification to Criterion 2.12 to address this inconsistent treatment of small TOP control centers: SDT Proposed Criterion 2.12. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above. APPA Recommendation for Criterion 2.12: Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above that performs the functional obligations of the Transmission Operator for 3 or more transmission lines operating between 200kV and 299kV. Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in Criteria 2.12 would be designated as Low Impact Rational: CIP Version 4 uses the bright line of 3 or more transmission lines operating at 300kV or above in criterion 1.7. From the weighted table in the draft 3 criterion 2.5, this would give a threshold of 1400 MVA between a Medium and Low Impact. The SDT acknowledges that transmission Facilities below 200kV are not applicable in the Medium Impact category. So it stands to reason that Control Centers that perform the functional obligations of the Transmission Operator for Low Impact Facilities should be designated as Low Impact. A threshold of three or more Transmission lines operating at over 200 kV and all Transmission Facilities operating at less than 200 kV will permit small TOPs to own and operate limited amounts of BES Transmission to connect local 115 and 138 kV networks to EHV BES Transmission Facilities, without imposing a disproportionate regulatory burden. APPA believes that this small but significant change would align the thresholds of all Control Centers and address the significant cost impact on small entities. APPA provided the following suggestion in the CIP V5 Draft 2 comments: APPA has focused our comments on the impact of the standards on small entities. We recommend that the SDT take a close look at the applicability and the requirements in all of the CIP Version 5 standards. Where the standards are applicable to small entities the SDT needs to account for the impact on small entities and only include those requirements if they are absolutely critical for the protection of the reliability of the BES. If these requirements must be included, then the SDT should allow for a small entity exemption process. Alternative Exception Process: APPA would offer the following alternative if the APPA recommendations for TOP thresholds are not adopted in a CIP-002-5 draft 4: APPA Recommendation for new Criteria 2.14: Each transmission Facility that its Planning Coordinator or Transmission Planner designates, and informs the Transmission Owner or Transmission Operator, should be excluded based on the following performance based exception process moving a TOP Control Center from Medium Impact to Low Impact: 1. If the TOP could demonstrate that another TOP had ultimate control or ability to isolate the excepted system, or 2. If the TOP has no ability to schedule voltage (reactive management), or 3. If it can be demonstrated that automatic or manual operation on the TOP system, including delayed clearing of category C events does not cause rating (including in the WECC region, TPL criteria) violations on neighboring TOPs. If the SDT provides reasonable changes to the treatment of small TOP control centers similar to the ones given to small BA and GOP control centers, APPA can recommend an affirmative vote on CIP-002-5. APPA also supports the comments of TAPS which asks the SDT to consider changing the applicability language in Sections 4.1.2.4 and 4.2.1.4 from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching...."

Individual

Nicholas Lauriat

Network & Security Technologies, Inc.
N&ST chose to abstain.
N&ST chose to abstain.
Group
Detroit Edison
Kent J Kujala
Detroit Edison's comment pertains to CIP-007-5 Part 2.2 & 2.3. Clarification surrounding the use of the term, "mitigation plan" would be valuable. To clarify Part 2.2 perhaps mention that the mitigation plan is intended as an internal document and not submitted to the Regional Entity. Detroit Edison finds CIP V5 well written, organized, easy to understand and easy to follow.
Individual
Steven Wallace
Seminole Electric.com
Individual
J. S. Stonecipher, PE
City of Jacksonville Beach, FL dba/ Beaches Energy Services
We appreciate the hard and excellent work of the SDT to significantly improve the CIP Standards and develop a prudent method to protect the Bulk Electric System from cyber attacks. Although we have several comments, only one comment is causing us to vote Negative for any of the Standards. CIP-002-5, Attachment 1, Bullet 2.12: The SDT added thresholds for Control Centers for small GOPs and small BAs to define a boundary between "Medium" and "Low" Control Centers, but no equivalent threshold for small TOPs, which is inappropriate. Why would a small control center controlling 1499 MW of generation be "Low" whereas a small TOP's control center for two 138 kV substations with only four 138 kV Facilities be "Medium"? We suggest that a threshold be added for small TOPs to distinguish between Medium and Low. The threshold can be design similar in concept to bullet 2.5, but including >100 kV and <200 kV Facilities with a score of 350. In this way, all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low.
These are issues that we believe should be fixed, but are not causing us to vote negatively. Zero-Defect solution doesn't get us all the way there: The helpful phrase: "shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented … policies" was added to many requirements to try and address the "zero-defect" problem. However, by choosing the active word "implement", the zero-defect problem is reintroduced. "Implement" means: "to fulfill, perform, carry out", which means that in order to prove that a policy was carried out, detailed evidence of the results of executing the policy is needed, reintroducing the zero-defect problem. We recommend replacing the word "implement" with "institute" which means "to set into operation" or "to bring into practice or use" for which the evidence would be less onerous (e.g., the policy itself and proof that it was instituted, such as procedures that support the policy) avoiding reintroduction of the zero-defect problem. CIP-002-5, R1: How is an auditor to verify identification of all BES Cyber Systems that are applicable to R1.1 and R1.2? We wait with interest on what the RSAW will look like. CIP-003-5, R4: The SDT seems to intend to address the zero-defect issue; however, by not associating the documentation of delegation contained in the 3rd sentence to the process of the first sentence, the goal is not accomplished and a strict reading of the requirement still includes a zero-defect problem of needing to document delegation for every delegation and delegation change within 30 days because there is more than one requirement embedded in R4. CIP-006-5, R1: The standard does not answer the question "how big does an opening in the Physical Security Perimeter have to be before is it deemed an access point"? It seems the SDT wants to use the 96 square inches used by some defense agencies, if so, we recommend explicitly stating that in the Standard. CIP-006-5, R1.9 and R2.3, CIP-007-5, R4.3, CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard, especially considering the Paragraph 81 effort which is seeking to retire requirements just like this. CIP-006-5, R2.1: The measure does not match the requirement. The requirement is for "continuous escorted access", the measure describes evidence at discrete points in time, not continuous. How is an entity to prove that a visitor was continuously escorted? Does this essentially mean video surveillance? Or written attestations of the person providing the escort?
Individual
Michael Falvo
Independent Electricity System Operator
The IESO supports all of 10 standards.
Section 1.1 under Compliance for each standard does not adequately address the Ontario compliance enforcement model. In Ontario the Market Assessment and Compliance Division (MACD) of the IESO is the compliance enforcement authority in Ontario. Suggest the section be revised to read: "1.1. Compliance Enforcement Authority: The Regional Entity, or in non-US jurisdictions an entity appointed by a local governmental authority, shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or

controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA." CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not acceptable to Canadians. Suggest the wording be revised to read: "One or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident and notify the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) or for Canadian entities the Canadian Cyber Incident Response Centre (CCIRC). Initial notification to the ES-ISAC or CCIRC, which may be only a preliminary notice, shall not exceed one hour from identification." Note that this needs to be vetted with CCIRC for their concurrence. For clarification, suggest adding "mimic display" to the second paragraph of CIP-007 R5 Rationale, resulting in "Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.)." For consistency, recommend changing CIP-008 R2 Part 2.1 from "at least once every calendar year, not to exceed 15 months" to "at least once every 15 calendar months" For clarity, recommend changing CIP-009 R1 Part 1.5 from "One or more processes to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery." to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

Individual

Glen Sutton

ATCO Electric Ltd.

AE thanks the SDT for addressing their concerns from the previous draft. AE requests that the SDT add a definition for the term Physical Access Point ("PAP"). This definition could be similar in structure to the definition of Electron Access Point and could read: "Physical Access Point ("PAP"): A designated entry point on the Physical Security Perimeter that allows passage through the Physical Security Perimeter and for which access is controlled."

Group

Southern Company

Antonio Grayson

CIP-006-5 RSAW-Page 2, text as written: For the purpose of this RSAW, "deficiencies" refer to possible non-compliances with the standard; not all deficiencies would become issues on non-compliance. Proposed text: For the purpose of this RSAW, "deficiencies" refer to possible non-compliances with the standard; not all deficiencies would become issues of non-compliance. Rationale For Not Supporting: Use of proper English. CIP-006-5 RSAW-Page 9, text as written: Evidence that the entity has physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days prior to the date of the compliance monitoring for: Proposed text: Evidence that the entity has physical access logs of entry of individuals with authorized unescorted physical access into each Physical Security Perimeter for at least ninety calendar days beginning with the date of the compliance monitoring for: Rationale For Not Supporting: Pragmatic implementation of physical security perimeters typically involves clean up of users prior to the compliance date. Prior to the compliance date, logs may have a combination of authorized users and some users who need to be removed before the compliance date. Logs for auditing should be required as of the compliance date, not before. CIP-006-5 RSAW- Rationale For Not Supporting: We recommend standard citation guidance in the RSAW that will be used across all regions.

Individual

Oliver Burke

Entergy Services, Inc. (Transmission)

We do not support CIP-010-1 R1, specifically R1.5 and R1.5.2, a test environment that models the baseline configuration of the BES Cyber System in a production environment is not always practical. In such cases, the requirement to document the differences between the baseline configuration and the test environment each time testing is executed would result in an unreasonable burden on the entities that would not justify the effort required. Suggest modifying the requirement to require documentation only of "material" differences between the baseline configuration and the test environment to avoid the documentation of differences lacking security implications. Maintaining a baseline configuration for every BES Cyber System is excessive and provides marginal benefit to the reliability of the BES cyber system.

Re-numbering of Existing Requirements - For situations where requirements are being moved from their CIP Version 4 Standard to a new Standard in Version 5, the old requirement number should be retired, and not re-used. For Example, the current CIP-007-4 R1, "Test Procedures" and its subparts, have been moved to CIP-010-1 R1.4 & R1.5. As a result, CIP-007-4 R2 "Ports and Services" has been moved to CIP-007-5 R1. As a result, documentation for Ports and Services that is currently identified with CIP-007 R2 will need to be identified with CIP-007 R1 beginning on the effective date of Version 5 of the CIP Standards. This may lead to confusion on the part of the Responsible Entities staff, as well as the audit staff when looking at evidence for a particular standard. Zero-Defects Issue The Background section of each draft Standard states that "The intent is to change the basis of a violation in those requirements so that they are not focused on whether there is a deficiency, but on identifying,

assessing, and correcting deficiencies." The Standard should be clear as to how this will work in practice to avoid uncertainty on the part of Registered Entities and auditors. If this should be read (and enforced) to mean that so long as there is a program that "identifies, assesses, and corrects deficiencies" related to the Requirement individual deficiencies are not violations of the Requirement, the Standard must explicitly say so. As written it is unclear whether individual minor deficiencies should be considered violations and self-reported if the program has been otherwise properly implemented but, for example, an entity suffered an equipment failure resulting in a temporary deficiency. BES Cyber Asset and BES Cyber System Categorization - Brightline Criteria – Medium Impact Ratings "Each BES Cyber System, not included in Section 1, above, associated with the following: 2. 1 Commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net Real Power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES Cyber Systems that meet this criterion are those shared BES Cyber Systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection. Each BES Cyber Asset or BES Cyber System, not included in Section 1, above, that if rendered unavailable, degraded, or misused would, within 15 minutes adversely impact one or more BES Reliability Operating Services " Comment: NERC Standard FAC-014-2 and its associated requirements (R5.1.1 and R5.1.3) states that 30 minutes to relieve the overload is sufficient. Similarly, Transmission Operators have 30 minutes to return the transmission system to within operating limits following an IROL violation under TOP-007-0 R2 or to return operations to proven reliable power system limits after entering an unknown operating state under TOP-004-2 R4. The new CIP requirements should utilize the same 30-minute period. It is inconsistent to have 30 minutes to address IROL violations but to measure adverse impacts on reliability under the CIP Standards on a significantly shorter time period. . Cyber Security – Personnel and Training R5 - Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented access revocation programs that collectively include each of the applicable requirement parts in CIP-004-5 Table R5 – Access Revocation. R5.1 – A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action (Removal of the ability for access may be different than deletion, disabling, revocation, or removal of all access rights). Comment: The Requirement does not distinguish between termination for cause and termination without cause (i.e. voluntary terminations, the end of contract periods, etc.). For termination without cause, the risk associated with not immediately initiating removal of access and completing such removal within 24 hours is minimal. Avoiding such minimal risk does not justify the administrative burden that expedited access removals this would impose. The 24 hour requirement should be modified to apply only to involuntary terminations or terminations for cause, with voluntary terminations added to R5.2 because voluntary terminations present no more risk than reassignments or transfers. R5.2 requires revocation by the end of the next calendar day.

Individual

John Shaver

Southwest Transmission Cooperative Inc.

CIP-002-5 R 2.12. The TOPs only have a bright-line criteria for medium and high impact. There is not a lot of difference between the requirements of a high or medium impact facility. However, there are tremendous differences in compliance requirements between low and medium impact. The way the standard is written today, all control centers owned by the TOP, no matter how small their footprint, will be classified as either a medium or high impact facility, resulting in financially burdensome compliance obligations. The BAs and GOPs have the ability if they are small to be classified as a low impact facility, and it seems appropriate to classify TOPs by applying similar size thresholds. Thank you.

Individual

Scott Bos

Muscatine Power and Water

MPW would like to thank the 706 SDT on their accomplishments in the CIP-002-5 – Attachment 1 – Impact Rating Criteria. The SDT was sensible in considering the Control Centers and backup Control Centers used to perform the functional obligations of the smaller Generator Operator (Item 2.11 of the Impact Rating Criteria) and Balancing Authority (Item 2.13 of the Impact Rating Criteria) that have less than 1500 MW in a single Interconnection to have a Low Impact Rating. This makes a great deal of sense because these entities do not pose a major reliability risk to the BES. However, for the small vertically-integrated municipal utilities that meet the Low Impact Rating Criteria for their Control Centers and backup Control Centers in their functional roles as Generator Operator and Balancing Authority under the 1500 MW threshold, this same type of granularity is not afforded to them in their functional role of Transmission Operator. This is NOT bright line criteria. The same methodology that brought about the 1500 MW threshold for smaller Generator Operators and Balancing Authorities should be applied for their functional role of Transmission Operator. For this reason, MPW cannot support CIP-002-5. The SDT needs to understand that not all Transmission Operators are created equally. Especially not the Transmission Operators at the small vertically-integrated municipal utilities. For these Control Centers and backup Control Centers of these small utilities to carry the Medium Impact Rating just because they are registered as Transmission Operators would be exceedingly burdensome and not equitable based on their very low impact to the reliability of the Bulk

Electric System.
As mentioned before, there should be a threshold level for the Medium Impact Rating of the Control Centers and backup Control Centers used to perform the functional role of Transmission Operator. The logical criteria to look at for determining a threshold level would be voltage. The criteria for Item 2.12 of the CIP-002-5 – Attachment 1 – Impact Rating Criteria should be rewritten similar to: Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator with Transmission Facilities operating above 200 kV and not included in High Impact Rating (H), above. Other options would be to have the Impact Rating Criteria of the Control Centers and backup Control Centers used to perform the functional role of Transmission Operator be based on the total mileage of Transmission lines or the number of Transmission lines operated by the Transmission Operator. MPW would support CIP V5 if there was consideration provided for the small vertically-integrated municipal utility performing the functional role of Transmission Operator that operate two 161 kV lines totalling 32 miles. It does not seem equitable that our neighbors operate several hundreds of miles of Tranmission, much of it at 345 kV, and have the same Medium Impact Rating.
Individual
Russ Schneider
Flathead Electric Cooperative, Inc.
I would support the proposed revisions if the BES definition is approved by FERC and implemented in its current form. However, without the BES definition being final it is premature to support the changes and potentiall burdensome on potentially non-BES protection systems that may be properly part of a local network or radial distribution system.
Individual
Allen D. Schriver
NextEra Energy
The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC's Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language ("in a manner that identifies, assesses, and corrects deficiencies" (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard's requirements. The proposed RSAW language regarding "deficiencies" and "self-reporting" does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase "in a manner that," which is itself prefaced by the words "shall implement," the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk

Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.

NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.

Individual

Yee Chou

American Electric Power

AEP does not support CIP-004, CIP-005 and CIP-010 for the following specific reasons: CIP-004 Requirement 3 involves performing personnel risk assessments (background checks) to employees and contractors alike. The current standards allow the entity to tailor their program, which could include different provisions for contractors versus employees if necessary. In addition, AEP has concerns that these and other changes have created requirements that are confusing and could be written clearer. CIP-005 Requirement 1.3 calls for requiring inbound and outbound access permission, including the reason for granting access, and deny all other access by default. Our major concern is regarding "outbound access permission". The target threat vectors to the BES Cyber Systems would be inbound to those networks and those attempts inbound into the networks need to be monitored and controlled. While there is the possibility that could be malicious code internal to these networks communicating, we think that tracking all outbound communication from one AEP trusted network to another AEP trusted network would more than double the monitoring that is required. In addition, the CIP standards have other controls to help monitor and detect the malicious code internal to the networks. CIP-010, Requirement 2.1 calls for monitoring at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1), and documenting and investigating detected unauthorized changes. AEP has internal processes for change management, which include approvals and controls, but AEP does not have tools for the detection of changes from the baseline for many systems. At this point in time, there are no tools commercially available that provide the necessary monitoring and tracking of changes of complex computer systems that indicate all of the changes made on top of the baseline configuration. This requirement might force us to perform cyber vulnerability assessment every 35 days which will consume major labor effort. In the meantime, we have additional comments to further improve clarity of the following standards: For CIP-002, Attachment 1, Sections 1.2 and 1.4 - change it to ".....assets that meet criterion.....2.6, or 2.9 (only if it is directly involved in the SPS functions). For CIP-003 AEP questions whether CIP-003 R1 and R2 match the parameters of efforts of team developed for Paragraph 81. The most elements required to be implement by policies are actually embedded in the remainder of the requirements in the other CIP standards. CIP-003 M1 – Does the wording of this measure infer that there has to be multiple procedures, whereas the requirement indicates that one or more procedures are valid? CIP-003 R2 – remove "shall implement" because a violation of a requirement might be a violation of the policy as well. For CIP-004, • R2 Language: o "…in a manner that identifies, assesses, and corrects deficiencies…" – does this mean that if we fail to meet all the requirements in the table that we can simply correct the problem and not self report? If so, we feel the language should be more definitive. o "…appropriate to individual roles, functions, or responsibilities…" – who defines what is / isn't appropriate? This looks like it leaves the auditors with a great deal of latitude to decide themselves what is appropriate / not appropriate. • Requirement 2.1.9 – suggest removal of this sub-requirement – otherwise, it would also apply to PCAs under the Applicable Systems o not sure what they mean by "cyber security risks" – seems rather vague and difficult to audit and subject to future CANs, interpretations, etc. o not sure what is meant by "interoperability" – seems vague and open to interpretation and a candidate for a future CAN, interpretation, CAR, etc. • Requirement 2.2 – If personnel change roles, it seems from the language in the requirement that they need to take the required training prior to assuming the new role. Is that the intention? If

so, this should be clarified in the requirement. • Requirement 3.3 – Suggest that the change rationale language match the language in the requirement. Specifically, "criteria" should be excluded – and only "process" be referenced. • Suggest removal of 3.3 and 3.4 – and roll them into 3.2. Also suggest that the reference to "contractors and service personnel" be rolled into the language of the R3 standard (i.e., make it applicable to both employees and contractors). Finally, note that 3.3 is completely redundant with 3.2. • Requirement 3.5 – suggest adding the word "calendar" before "years" For CIP-006, • R1.5 – suggest they remove the 15 minute maximum limit on the alarm /alert – leave the language as simply "Issue an alarm or alert in response to detected unauthorized circumvention of access through a physical access control point into a Physical Security Perimeter." • R1.7 – suggest change to simply: "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System." • R1.8 – suggest they add "initial" before "entry" in the last sentence – this would make it align with R2.2 for visitors For CIP-008, • 4.1.2.3 – attachment 1 of CIP-002 would probably limit the impact to DPs (most would fall below medium) • R1.1 – definition of Cyber Security Incident – difficult to determine intent of potential attacker – "suspicious" is rather vague and would leave it to the entity to define for itself • R1.2 -- "…which may be only a preliminary notice, shall not exceed one hour from identification determination" – we question the value of having this time limit (but we realize it is in the FERC Order 706) – would require that entities install a time stamp step in their incident response process to indicate when something was identified as reportable and then retain all this information in records to prove compliance to auditors – seems to be a candidate for Paragraph 81… For CIP-009, • R1.3 - There should be consistency in the applicability to ensure consistency across the different standards. For example, some indicate "with External Routable Connectivity" or "without External Routable Connectivity" if it is not specified which apply? • R1.4 - Suggest removing "...and to address any backup failures." This may lead the reader to the notion of having another pre-determined plan to account for unknown issues during the backup. • R1.5 - The requirements could put the Registered Entity into a "Catch-22" scenario. They could try to comply with the requirement by saving logs, which might impede recovery. Who is given the discretion of making the determination of which approach should have been taken? It is likely that the auditor will have their own perspective after the fact which may not align with the thinking of the Registered Entity during the event. Poorly worded…. • R3.1 - "After completion of a recovery plan test or actual recovery and not to exceed 90 calendar days after completion..." should be stated at "After completion of a recovery plan test and not to exceed 90 calendar days after completion..." A lessons-learned activity should not be required for every failure of equipment in the field. For CIP-010, • R1.1 - AEP suggests to add "software package", not just "software". AEP would also ask clarification that these "items" are current, not any historical ones. • R1.3 - Should it be 35 calendar days which will be consistent with other requirements? • R1.5 - In the Measures, "description of how any differences were accounted for" is unreasonably challenging. It's not possible to scale this to any large number of BES Cyber Assets. • R2.1 - How do we detect "unauthorized changes"? Is this calling for CVA every 35 days? • R3.2 - The comment for R1.5 applies here. • R3.4 - Are the vulnerabilities identified in this assessment considered as "violations"? For CIP-011, • R1.2 – It is suggested that the last bullet for the Measures for Part 1.1 be added to Part 1.2. The following is the specified language "Repository or electronic and physical location designated for jousting BES Cyber System Information in the entity's information protection program." • CIP-011 R2 should contain the phrase "in a manner that identifies, assesses and correct deficiencies." For Definition, • AEP Recommends that data center (used in the Control Center definition) be a defined term. • Cyber Assets - For the definition of Cyber Assets, how does the wiring between Cyber Assets come into play? • Electronic Access Point ("EAP") - AEP recommends that definition be changed to: o "A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication..." From: o "...Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter." • Intermediate Device - Does this interpretation lead to the solutions like jump-hosts or do systems like SecureID or CISCO ACS qualify as Intermediate Devices? Also, as written would this definition lead Registered Entities to not have the Intermediate Devices in another ESP? • Reportable Cyber Security Incident - - This definition if very vague and AEP would develop its own definition.

SDT has done a good job further clarifing these standards. AEP is ready to provide full support once the issues in CIP-004, 005 and 010 are addressed properly.

Group

CenterPoint Energy

John Brockhan

Definitions – CenterPoint Energy does not support the definition proposed for Dial-up Connectivity, "A data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link." The Company prefers a definition that is more aligned with what was previously provided in CIP-related FAQs, "any temporary (non-permanent), interruptible or not continuously connected communication access to a Critical Cyber Asset from any remote site. Using a modem over a land line, wireless technology, or VPN using a routable protocol to connect to a Critical Cyber Asset from one or more locations or by one or more users are examples of dial-up accessible access. Access to a Critical Cyber Asset via a permanent communication connection from a specific computer over a dedicated communication circuit would not be considered dial-up accessible access." There are specific concerns with the proposed definition's lack of consideration for the direction of communications versus the phrase "to connect to a Critical Cyber Asset from one or more locations" provided in the FAQs. Also as previously submitted, CenterPoint Energy believes "was an attempt" in the definition of "Cyber Security Incident" is vague and seeks clarification on how such an attempt

would be determined. An alternative would be to delete the phrases "or was an attempt to compromise" and "or was an attempt to disrupt". CIP-002 – CenterPoint Energy also still has significant concerns with criteria 2.5. As currently defined, the values force a label of critical on non-critical Facilities as proven by intricate studies performed by transmission planning engineers. CenterPoint Energy recommends the values be revised as follows: Voltage Value of a Line 200 kV – 399 kV – Weight Value per Line - 800; Voltage Value of a line 400kV to 499 kV – Weight Value per Line – 1300. CIP-003 – The reference to "CIP-002-5, Requirement R2" should be to Requirement R1. CenterPoint Energy suggests that the phrase "low impact" be used in R2 as "high impact" and "medium impact" is used in R1. For example, the requirement would be as follows: "Each Responsible Entity for its low impact BES Cyber Systems shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented cyber security policies that address the following topics, and review and obtain CIP Senior Manager approval for those policies at least once every 15 calendar months: [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]". CenterPoint Energy questions the addition of the "zero defect language" to requirement, R4. (The Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates. These delegations shall be documented, including the name or title of the delegate, the specific actions delegated, and the date of the delegation; approved by the CIP Senior Manager; and updated within 30 days of the initial delegation and any change to the delegation. Delegation changes do not need to be reinstated with a change to the delegator. [Violation Risk Factor: Lower] [Time Horizon: Operations Planning]) The Company believes that the requirement is binary in that delegations are assigned or not. CIP-006 – CenterPoint Energy questions the addition of the "zero defect language" to requirement, R1. (Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented physical security plans that collectively include all of the applicable requirement parts in CIP-006-5 Table R1 – Physical Security Plan. [Violation Risk Factor: Medium] [Time Horizon: Long Term Planning and Same Day Operations].) The Company believes that the requirement is binary in that a documented physical security plan exists or not. CenterPoint Energy recommends that the Applicable Systems in R1.1 be revised from "Medium Impact BES Cyber Systems without External Routable Connectivity" to" Medium Impact BES Cyber Systems" as that has been the label for Medium Impact BES Cyber Systems not having External Routable Connectivity. (Unless there is a difference between the terms "Medium Impact BES Cyber Systems" and "Medium Impact BES Cyber Systems without External Routable Connectivity") CIP-007 – CenterPoint Energy suggests the following alternate wording for requirement part, 5.2: "Identify and inventory all KNOWN enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s)". CenterPoint Energy still prefers that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for the Patch Management requirements, R2.1 – R2.4. The Company understands the comments of the SDT; however, believes that a combination of no external routable connectivity, frequency of access to medium impact facilities, and policies reduces the risks to those facilities from the insider that would introduce threats ("thumb drives, laptops, smart phones") into the environment to an acceptable level. While devices with no external connectivity may have some physical access risks associated with the use of thumb drives, laptops, etc., the fact that they are isolated from other BES devices must be considered when addressing appropriate protections. The lack of external connectivity reduces the risks to that isolated device; therefore, the risk to the BES is minimal. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. Alternatively, CenterPoint Energy requests that the timeframes for requirement parts, 2.2 and 2.3 be revised to 90 days for Medium Impact BES Cyber Systems. CIP-008 – CenterPoint Energy is concerned with the reasonableness of the 1 hour reporting requirement in part 1.2 and recommends that the SDT increase the timeframe. CenterPoint Energy still believes that Part 2.2 is too prescriptive as it relates to documenting deviations and recommends that the SDT remove "documentation of deviations" as deviations in a sense should be captured in lessons learned (i.e. after-the-fact versus during critical time). CenterPoint Energy requests that the SDT add "except in CIP Exceptional Circumstances" and a sentence related to impeding recovery as noted in CIP-009 Part 1.5 (Data preservation should not impede or restrict recovery). CIP-009 – CenterPoint Energy is not sure of the placement or intent of Requirement Part 1.5 and requests that the SDT consider revising or moving this requirement to CIP-008. CenterPoint Energy requests clarification on the intended frequency of part 1.4 ("verify the successful completion of the backup processes") and the reference to a "representative sample" in part 2.2. CIP-010 –CenterPoint Energy still prefers that the SDT add "with External Routable Connectivity" to the Medium Impact applicability to the requirements of this standard. No external routable connectivity, frequency of access to the facilities, and policies reduces the risks to those facilities from the insider that would introduce threats into the environment to an acceptable level. Additionally, physical security is adequate mitigation from the external threats as once physical security is breached; there are other immediate and evident concerns that do not involve BES Cyber Systems. CenterPoint Energy does not perceive how adding "with External Routable Connectivity" to the requirements explicitly conflicts with the FERC directive (elimination of the blanket exemption for non-routable connected cyber systems) as there are other standards and requirements that clearly demonstrate acknowledgement and response to the directive. Alternatively, the Company requests that requirement part, 1.3 be revised to 90 days for Medium Impact BES Cyber Systems. CenterPoint Energy proposes that the associated timeframe for requirement part, 1.3 (For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.) be updated to 90 days instead of 30 days. CenterPoint Energy proposes that the SDT

change the timeframe associated with requirement part, 2.1 to 90 days. CIP-011 – CenterPoint Energy recommends that the SDT add "with External Routable Connectivity" to the Medium Impact applicability for this standard.
CenterPoint Energy recommends the above changes for an affirmative vote on all ballots.
Individual
Brett Holland
Kansas City Power & Light and KCPL-GMO
N/A
It is essential that the standards contain everything that is required and to not intentionally or inadvertently include requirements by reference in other documents. The standards should stand on their own, without reference to other documents that introduce interpretation for requirements without use of established processes approved in the Rules of Procedure. Further, all definitions must be captured in the definitions document. We encourage the removal of "rationale" statements throughout as requirements do not consistently support the list. To prevent misinterpretation, "Electronic access controls for routable protocol connections and dial-up connectivity external to the ESP" is suggested for CIP-003 R2-2.3. In CIP-004 R5.3, change "by the end of the next calendar day" to "within 30 calendar days". In CIP-007 R4.4, the "summarization" and "sampling" components are too broad. We encourage specificity in all measures. Additionally, the term "undetected" is unclear and confusing. Clarification, such as "logged but not previously selected for alerting or alarming" could be helpful. Lastly, CIP-010 R1.5.2 should specify to what level the differences must be documented between the test environment and the production environment to ensure cost benefit for the level of investment. In addition, KCP&L endorses the comments filed by SPP RTO.
Group
Southwest Power Pool Regional Entity
Emily Pennel
Implementation Plan: (1) Compliance with CIP-003-5/R2 upon the 13th calendar quarter is excessively long; especially considering the requirement is to draft a small number of policies. (2) Continued insistence that Version 4 will not see the light of day sends the wrong message to the registered entities that will face violations and possibly stiff penalties if they heed this message and Version 4 does go into effect. Given past history, it is exceptionally unlikely that FERC will approve Version 5 prior to the Version 4 effective date. The only way to realistically obviate Version 4 and retain Version 3 is for FERC to rescind Order 761. (3) The compliance expectation for CIP-002-5/R2 needs to be qualified with "in sufficient time to be able to ensure the identified BES Cyber Systems are compliant with the applicable requirements of CIP-003-5 through CIP-009-5 and CIP-010-1 through CIP-011-1 as of the effective date of these standards as adjusted by this implementation plan." (4) To preclude record keeping issues, compliance with CIP-004-5/R4.2 should be required on or before the effective date. (5) To preclude initial errors, compliance with CIP-004-5/R4.3 and R4.4 should be required on or before the effective date. (6) The compliance statement for CIP-006-5/R3.1 should require testing within 24 months of the previous test for physical access controls subject to previous versions of the CIP standards and only allow 24 months from the version 5 effective date for newly in-scope physical access controls. (7) Including CIP-008-5/R3.1 in group 6 of the implementation plan is illogical as this activity is triggered by a test or an actual incident. (8) Including CIP-009-5/R3.1 in group 6 of the implementation plan is illogical as this activity is triggered by a test or an actual recovery event. (9) Compliance with CIP-010-1 (not CIP-010-5)/3.1 should be required on or before the effective date for any new Cyber Asset not subject to a previous version of the CIP standards. This is consistent with CIP-010-5/R3.3 that requires an active vulnerability assessment for any new Cyber Asset prior to placing the Cyber Asset into production. (10) CIP-011-1 (not CIP-011-5)/R1.3, included in group 6 of the implementation plan, does not exist. (11) CIP-009-5/R2.3 is included in both group 6 and group 7. (12) Compliance with CIP-010-1 (not CIP-010-5)/3.2 should be required on or before the effective date for any new Cyber Asset not subject to a previous version of the CIP standards. This is consistent with CIP-010-5/R3.3 that requires an active vulnerability assessment for any new Cyber Asset prior to placing the Cyber Asset into production. (13) Group 8 is not necessary as this requirement is already articulated in CIP-004-5/R3.5. If retained, the expectation should be modified to require an updated PRA "within 7 years of the anniversary date of the last personnel risk assessment that was performed pursuant to a previous version of the CIP Cyber Security Standards." (14) In the "Previous Identity Verification" section, the reference to CIP-004-5/R4.1 is illogical. The reference is more likely CIP-00405/R3.1. (15) In the "Scenario of Unplanned Changes After the Effective Date" table, the last scenario (identifying the first medium impact or high impact BES Cyber System) needs to be clarified whether this applies to the first BES Cyber System as a location/facility or the first BES Cyber System identified overall (i.e., the Responsible Entity had no previously identified BES Cyber Systems whatsoever). (16) Under the weakest link principle, the CIP-004-5/R4 Access Management Program and the CIP-004-5/R5 Access Revocation requirements in the Applicability Reference Tables should also apply to Protected Cyber Assets. (17) In the Applicability Reference Tables, Physical Access Control Systems should be protected by an ESP-like perimeter in the same manner they are required to be protected under CIP Version 3. (18) In the Applicability Reference Tables, Electronic and Physical Access Control or Monitoring Systems should be subject to CIP-005-5/R2 Remote Access Management. Definitions of Terms: (1) Throughout the definitions, there continues to be references to "would" (e.g., would within 15 minutes… or would effect…). The criteria need to be prospective. From a risk perspective, if

something "could" happen, then entities should assume that under the right conditions it "would" happen and require the protective controls to be implemented. The use of "would" implies certainty and registered entities may argue over that distinction in determining certain BES Cyber Systems are not subject to the CIP standards. The definitions need to use the phrase "could" and not "would". (2) Allowing a CIP Exceptional Circumstance may not always be appropriate in the instance of an "imminent or existing hardware, software, or equipment failure." This provision allows a Responsible Entity to declare a "CIP Exceptional Circumstance" for petty issues that do not place the reliability of the BES at risk in order to bypass the requirements of the CIP standards. (3) The reference in the definition of Control Center to controlling the BES in real-time allows a Responsible Entity to take an entity-centric view and argue that while they may be controlling multiple facilities and performing the RC, BA, and/or TOP functions, they are not "controlling" the BES. The definition should remove the "BES control" reference and simply apply the definition to RC, BA, and TOP functions performed. (4) The definition of Cyber Security Incident should also apply to Protected Cyber Assets, EACMS, and PACS. (5) The definition of Electronic Security Perimeter allows the Responsible Entity to serially connect certain Cyber Assets (e.g., Digital Protective Control Devices) to a communications processor that, in turn, communicates to other Cyber Assets using a routable protocol, and in doing so declare that the DPCD do not need to reside within the ESP and therefore are not subject to the CIP standards. (6) The definition of Reportable Cyber Security Incident is too broad. Detected malware might not have disrupted or compromised a reliability task, but it has compromised the Cyber Asset where the reliability task is performed. Such malware could compromise the task in the future upon instruction from a command and control system with which it is communicating. Any malware infection of an in-scope Cyber Asset should be reported. General Comments Applicable to Multiple Standards: (1) The intent of a number of requirements is to change the basis of a violation so that the focus is on identifying, assessing, and correcting deficiencies. While the intent is noble and overall beneficial, there are two issues that need to be considered and addressed. First, at some point, the number of deficiencies found and corrected becomes excessive and is indicative of a poor or non-existent compliance program. The standards do not address the point at which "found, fixed, no harm, no foul," especially for recurring failures with the same requirement, becomes a finding of overall non-compliance and is subject to a violation. Without boundaries, the Responsible Entity could continue to falter, do nothing significant to correct the underlying deficiencies, and hide behind the "find, fix, and essentially move on" approach. Even the Find, Fix, and Track (FFT) enforcement program has provisions for taking note of repeat incidents and elevates the FFT to a prosecuted violation for repeated failures. Second, there is no apparent requirement for the Responsible Entity to document the failure and the actions taken to correct and prevent further recurrences, similar to a mitigation plan for a violation under today's standards. Without required documentation and an expectation of audit review, Compliance Enforcement Authorities will have no basis for judging the effectiveness of the audited entity's internal compliance program. This is of significant concern for the CIP-007-5 requirements as they have the greatest impact on actually protecting the BES Cyber Systems. (2) There are a number of requirements that require a program or procedure to be documented, or for the Responsible Entity to have a method to perform some task, but do not explicitly require implementation. While implementation is implied, FERC found this to be a shortcoming in the CIP Version 1 standards and required the standards to be modified to explicitly require implementation of the documented process. To preclude a similar order by FERC in addressing the Version 5 standards, the language should be modified now to address and remedy the issue. (3) the accompanying guidelines contain significant valuable information and explanations of intent. Some of this guidance needs to be incorporated into the requirement itself. As Registered Entities are quick to point out, guidance is not an auditable requirement. If the guidance expresses an expectation, that expectation needs to be explicitly stated in the requirement. (4) Stated intervals in the standards are not consistent. Most "annual" requirements have been modified to require the activity at least once every 15 months. There are still a few requirements that require the event to occur each calendar year with no more than 15 months interval between activities. From both entity compliance and an audit perspective, requiring an activity to occur at least every calendar year with a defined maximum interval is easier to program and monitor. CIP-002-5: (1) Similar to the Definition of Terms, this standard and attachment use the term "would", which implies an arguable certainty. The standard needs to take a prospective view and use the term "could", requiring the Responsible Entity to assume that the criteria will come to fruition and in doing so properly identify BES Cyber Assets that require protection under these standards. (2) The examples of Physical Access Control Systems used within this and other CIP Version 5 standards needs to include the workstations used to provision physical (e.g., badge) access rights and/or are used by security personnel to monitor for and receive physical security alerts. Excluded from this definition are workstations that create the physical badge as long as that workstation and associated equipment only create the badge and are not used to provision access rights associated with the badge. (3) The use of the term "considers" in Requirement R1 leads to the same confusion as exists with the existing CIP-002-3 standard as some entities will argue that "consider" does not mandate a required subsequent action. The requirement should be restated as "For each asset type enumerated below, each Responsible Entity shall:". (4) The assertion in Requirement R1.3 that the entity is not required to produce a list of low impact BES Cyber Systems renders this requirement not auditable for accuracy or completeness. To demonstrate that all high and medium impacting BES Cyber Systems have been properly categorized, the entity must be prepared to produce a list of all BES Cyber Systems that were evaluated, the remainder of which represent the low impacting BES Cyber Systems. The entity must also be prepared to demonstrate the minimal requirements applicable to low impacting BES Cyber Systems have been properly implemented, also requiring a list of impacted systems. CIP-002-5/Attachment 1 (Impact Rating Criteria): (1) the 3000 MW minimum specified in criterion 1.2 is excessive and does not appropriately reflect the potential risk a network-connected Balancing

Authority has not only upon its own service area but also upon the rest of North American BA, TOP, and RC registered entities with which it is directly or indirectly connected via the ICCP communication networks. (2) The 200 kV floor specified in criterion 2.5 does not adequately consider the risk to the BES imposed by large regional areas that are predominately sub-200 kV. The 2011 Southwestern blackout demonstrated just such a risk, even experiencing issues at sub-100 kV voltage levels that contributed to the disturbance. The BES is defined as 100 kV and above and the criterion needs to consider all of the BES in some manner. (3) The 1500 MW minimum specified in criterion 2.13 is excessive and unreasonably excludes a significant number of Balancing Authorities from meaningful participation in protecting the BES from cyber attack. Given that all BAs, TOPs, and RCs are interconnected via the ICCP links, these excluded Balancing Authorities could easily be the initial vector to attack the entire North American grid by exploiting trusted communication paths and exceptionally vulnerable ICCP systems to gain access to and compromise BES Cyber Systems essential to the reliability of the BES. Establishing criteria that effectively eliminates significant numbers of interconnected control centers fails to address the specific concerns outlined in both Order 706 and Order 761. (4) The use of the terms "critical" and "initial system restoration" in criterion 4.4 is problematic. Initial system restoration is not a defined term and registered entities have regularly argued that none of their resources are critical as they have many options from which to draw upon. The criterion needs to reflect the language and system restoration considerations found in EOP-005-2, Requirement R1, recognizing that it is not the role of the CIP compliance auditor to determine either the state at which initial system restoration is complete nor the viability of the EOP-005 system restoration plan when auditing this requirement. The criterion must provide certainty to both the Responsible Entity and the auditor and the current language falls short in that regard, suffering the same issues seen today in CIP-002-3. (5) The Low Impact Rating criteria needs to include automatic load shed systems that do not shed sufficient load to meet criterion 2.10. CIP-003-5: (1) The language of R1 and R2 could be improved by requiring one or more documented cyber security policies that "collectively" address the enumerated topics. (2) Requirement R3, as written, is not auditable and does not support the auditing of other requirements which require CIP Senior Manager approval. Identifying the CIP Senior Manager solely by name does not address the instances where there are multiple employees by that same name. The appointment must be able to uniquely identify the appointed CIP Senior Manager. Even an appointment by position title, as permitted for delegations of authority, is a superior approach to a name-only appointment document. Additionally, the absence of the effective date renders the 30-day update requirement not auditable and additionally precludes the verification of proper authorization where the approval of the CIP Senior Manager is required. (3) Similar to Requirement R2, an appointment of a delegate by name only does not uniquely identify the person being delegated authority. Delegating by position title is a far superior approach, especially as the delegation is permitted to succeed changes in both the CIP Senior Manager and the delegate him or herself. (4) In the discussion of possible controls to consider, the use of "ingress and egress" in section 1.2 is a physical access term being applied to logical access. "Login and logout" or "session initiation and termination" would be more appropriate language. Additionally, visitor management controls is conspicuous by its absence from the suggested controls in section 1.3. CIP-004-5: (1) It is not clear if the training required by Requirement R2 extends to contractors and vendor support staff. The extension is implied, but the requirement needs to be specific. The accompanying guidance is specific, however like the CIP standards FAQ today, guidance is not an auditable requirement. (2) It is not clear if the evaluation process specified in Requirement R3, Part 3.3 includes an expectation of clearly defined evaluation criteria for approval/disapproval of the access request. (3) It is not clear if the verification process specified in Requirement R3, Part 3.4 expects the Responsible Entity to perform the evaluation or permits the contractor or service vendor to perform an evaluation using its own criteria with an assertion to the Responsible Entity of compliance and acceptability. At a minimum, the Responsible Entity should be required to review and concur with the evaluation process and criteria used by the contractor or service provider if the entity is permitted to rely upon the assertion of the third-party provider. (4) Requirement R3, Part 3.5 needs to be clarified by replacing the phrase "within the last seven years" (that carries a similar ambiguity as the term "annual") with the phrase "on or before the seventh anniversary of the previously conducted personnel risk assessment." (5) Requirement R4, Part 4.2 should at least verify authorization records against actual access to detect any instance where access was erroneously granted or not revoked as expected. Verification of specific access rights is not required by the quarterly review, but verification of overall granted access is important and cannot be accomplished solely by a documentation review. (6) Requirement R5, Part 5.2 should be modified to revoke access by the end of the next "business" day as opposed to the next "calendar" day. As the revocation results from a reassignment or transfer, and not a termination for cause, the potential risk does not mandate a next calendar day revocation. CIP-005-5: (1) Requirement R1, Part 1.5 needs to include an explicit requirement for real-time monitoring and/or alerting upon detection of known or suspected malicious communication. Registered Entities will read the requirement explicitly and as written can make an argument that there is no requirement to monitor for or alert upon detected malicious traffic. CIP auditors have already encountered entities that deploy Intrusion Detection Systems but only monitor the IDS during normal business hours, or occasionally review the logs for events of interest. Simply detecting malicious traffic, with or without logging, does not address the immediate risk posed by the activity. CIP-006-5: (1) Requirement R1, Part 1.3 may not be responsive to FERC Order 706. The language of the requirement could be improved by adopting the "layered and complementary security procedures" language found in Paragraph 573 of Order 706 with a focus on defense in depth as articulated multiple times in the Order. The concern expressed by FERC staff at the time of the order was that the complementary controls be designed such that the failure of a single control did not result in a failure of the complementary control yielding uncontrolled access. In that light, the comment in the guidance section for this

requirement that states two-factor authentication would be acceptable is not appropriate. Instead, a series of access controlled doors or even a locked fence gate in combination with the control house at the substation could be acceptable. (2) Requirement R2, Part 2.2 as written could allow a logged entry/exit to span multiple days with no documentation of a significant gap in access. While the intent is to not require the visitor to log out and back in when briefly stepping out of the PSP (such as to retrieve tools or repair parts from the visitor's vehicle), the requirement should expect the visitor to sign out when departing the premises, such as going to lunch or overnight. (3) The 24 calendar month interval specified in Requirement R3, Part 3.1 is still excessive for normally occupied facilities such as a primary control center. This is especially true when the physical security controls are protecting high impacting BES Cyber Assets. CIP-007-5: (1) Requirement R2, Part 2.1 requires the Responsible Entity to identify a source or sources that the entity will track for the release of cyber security patches. The corresponding guidance suggests that the third-party SCADA system vendor is an appropriate source for patch availability notification. The ability of a Responsible Entity to wait until a SCADA system vendor "certifies" a patch before requiring the Responsible Entity to begin the assessment and follow-on patching process introduces unnecessary risk to the BES. There is a significant difference between assessing a patch for applicability and assessing a patch for installability. An applicable patch may be found to be incompatible with the third-party vendor's systems, would not be certified, and should not be installed. That does not mean the vulnerability being addressed by the patch should not be mitigated, rather it is incumbent upon the Responsible Entity to protect its systems in a timely manner. The Responsible Entity needs to select a patch availability source that is timely, including the original patch provider and well recognized general information providers like US-CERT, SANS @Risk, and nCircle. There is no harm in then waiting for the SCADA vendor to certify the patch before installing it, but the Responsible Entity is at least aware of the vulnerability, can assess the risk, and take appropriate interim action. (2) Requirement R2, Part 2.3 requires the Responsible Entity to either install the patch within 35 calendar days or simply create or update a mitigation plan. There are no boundaries of what is acceptable in a mitigation plan, no expectation of justifying the decision, and no requirement for CIP Senior Manager approval, thus allowing an entity to completely avoid the requirement to patch a critical system by creating an illogical plan with unreasonable milestone dates. The need to wait for a scheduled outage at a field asset is well understood. Allowing an entity to determine patches will only be installed when the control center server is replaced (typically every four years), as has been seen during a CIP audit, is unreasonable and poses significant risk to the reliability of the BES. This requirement does not require compensating measures appropriate to the vulnerability to be put into place until the patch is installed, thus furthering the potential risk. In effect, the provisions of this requirement have the potential of creating a paper exercise with little value, with an expectation that the CIP auditor simply accept the documented plan without comment. (3) Requirement R2, Part 2.4 furthers the inaction of the Responsible Entity by requiring the entity to follow the potentially illogical plan that the entity designed to avoid having to patch in the first place. As long as an extension of the plan is not required, there is still no CIP Senior Manager or delegate approval required. (4) Requirement R3, Part 3.1 requires the Responsible Entity to "deter, detect, or prevent" malicious code. As written, the entity has a choice of options, including an option to simply detect with no timeframe boundaries for when or how often the detection process must run or for monitoring the detection process itself. Simply detecting malware potentially places the BES at risk. The risk is mitigated proportionate to the time elapsed between the actual compromise, the detection, and the realization that malware has been detected. (5) Requirement R3, Part 3.3 requires the anti-malware updating process to address testing of the signature or pattern file. This requirement needs to be clarified. A number of Registered Entities have taken the position in the past that they address this aspect of the existing CIP Version 3 requirement by relying upon the vendor to test before release. (6) Requirement R4, Part 4.2 needs to be clarified whether the alert needs to be generated in real-time with automatic notification or if the alert can be generated by a long after-the-fact manual review of security event logs. (7) RequirementR4, Part 4.3 needs to be clarified whether original source logs must be retained or if post-log analysis summaries are sufficient. (8) Requirement R4, Part 4.4 needs to be clarified that the review of a summarization or sampling of logs is not acceptable as the primary means of log analysis and alert generation. The purpose of the manual review is to achieve a level of comfort that the log analysis tool is properly configured and is not missing important security events. A random sample review of logs otherwise runs a significant risk of completely missing security events that pose potential risk to BES reliability. (9) The term "generic account types" used in Requirement R5, Part 5.2 is not defined and has not been well understood to date by Registered Entities. (10) Requirement R5, Part 5.4, needs to be clarified that it pertains to active user accounts. There is no value to changing a password for an inactive or disabled user account until such time as the account is enabled. The requirement should also be clarified to require the initial password change prior to placing the BES Cyber Asset into service. (11) Requirement R5, Part 5.5 is limited to "password-only" authentication. The scope is too narrow and needs to include any use of a password for interactive access, even if part of a multi-factor authentication. This also needs to include user accounts that are capable of being used interactively even if the intended use is only programmatic (e.g., an FTP account). (12) Requirement R5, Part 5.7 should be clarified to establish an upper bound (or maximum number of attempts) to generate an alert or initiate an account lockout. CIP-008-5: (1) Requirement R2, Part 2.1 needs to be clarified whether a Cyber Security Incident response plan with multiple scenarios requires each scenario to be tested at least once per calendar year. (2) Requirement R2, Part 2.2 suffers a "catch-22." The requirement expects use of the Cyber Security Incident response plan when responding to a Reportable Security Incident, however execution of a step in the Cyber Security Incident response plan is required in order to determine if the incident is reportable. CIP-009-5: (1) Requirement R2, Part 2.1 needs to be clarified whether a recovery plan with multiple scenarios requires each scenario to be tested at least once

every 15 calendar months. (2) Requirement R2, Part 2.2 requires a "representative sample" of information used to recover BES System functionality to be tested. This requirement needs to be clarified. Does the requirement apply to only some or every Cyber Asset comprising a BES Cyber System? What is the minimum expectation of "representative sample?" Would a single file be sufficient, or is a partial or full restoration required (e.g., for one of multiple operator workstations)? (3) Requirement R2, Part 2.3 needs to be clarified whether a recovery plan with multiple scenarios requires each scenario to be tested at least once every 36 calendar months. CIP-010-1: (1) The term "active vulnerability assessment" used in Requirement R3, Parts 3.1, 3.2, and 3.3 needs to be formally defined. While the accompanying guidance attempts to define the use of the term, the guidance is not binding and is not auditable. (2) A paper vulnerability assessment, basically a documentation review, does little if anything to identify vulnerabilities present on a BES Cyber System. This requirement represents a significant step backward from the cyber vulnerability assessments required under the Version 3 CIP standards. CIP-011-1: (1) Requirement R1, Part 1.2 needs to be clarified to ensure protection and secure handling of BES Cyber System information when in transit both electronically and physically. For example, the entity should be required to protect such information when the media it resides on is being shipped by commercial carrier to a new location.

While certainly a major step in the right direction, many requirements provide no boundaries of acceptability, thus making any compliance audit highly subjective. No doubt, the auditors are qualified to subjectively determine when compliance is "good enough" but entities will likely disagree. This is going to cause significant issues down the road when the standards go into effect and compliance must be demonstrated.

Individual

Nazra Gladu

Manitoba Hydro

We don't support certain requirements with comments as follows: Global comments: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies…" is difficult to interpret and therefore creates uncertainty as to what is required. The Background section of the standard indicates that the SDT intended the phrase to be aimed at "deficiencies in the implementation of certain requirements". However, it is inconsistent to require "implementation" in a manner that does not require implementation, leaving the interpretation of this standard unclear. It also appears that the SDT did not want implementation failures to constitute violations. However, as drafted, the standard can still be interpreted to require an entity to implement its processes. It simply places an additional obligation on a Responsible Entity to detect and correct implementation failures. If the SDT wishes to eliminate violations for failure to implement a process, then there should be a separate requirement to detect, assess and correct deficiencies in implementation. Attachment 1 1.2-2), 1.3 & 1.4: It is not reasonable that a control center is classified as (H) High Impact Rating asset if it controls one Medium Impact Rating assets as defined in Section 2. As written, e.g., if a utility Control Center only controls a single Medium Impact Rating transmission or generation asset and one Low Impact Rating transmission or generation asset, its Control Center becomes a (H) Control Center that has the same classification as a large Transmission Operator Control Center facility! We suggest changing from "includes control of one or more of the assets..." to "includes control of two or more of the assets…" in Section 1.2-2), 1.3 and 1.4. Attachment 1 1.4: It is not reasonable that the GOP control centre has different MW threshold from the BA control centre. We suggest rewording 1.4 as following: "Each Control Center or backup Control Center used to perform the functional obligations of the Generation Operator: 1) for generation equal to or greater than an aggregate of 3000 MW in a single Interconnection, or 2) for one or more of the assets that meet criterion 2.3, 2.6, or 2.9." Attachment 1 2.5: We suggest the following rewording the first sentence for increased clarity: "Transmission Facilities operated between 200 kV and 499 kV if the BES Transmission Lines that are operating between 200 kV and 499 kV at a single station or substation have an "aggregate weighted value" exceeding 3000 according to the table below and the single station or substation is connected to three or more other Transmission stations or substations that are each operating between 200 kV and 499 kV." Attachment 1 2.9: Please clarify what is called "automated switching System" and why the 'System' is capitalized. Attachment 1 Section 3: The numbering 4.1-4.3 should be changed to 3.1-3.3. CIP-003-5: R1: Requirement R1 does not achieve its objective of ensuring that a cyber-security policy is kept" up to date" (as stated in the preceding rationale) as it only requires a Responsible Entity to periodically review the policy, but not revise the policy if it does not reflect actual practice. Furthermore, if the review of a policy every 15 months was intended to allow a Responsible Entity to revise a policy after changes in practice have already occurred, this implies that policies need not always be" up to date". It also implies that Responsible Entities need not implement their actual policies as worded, which creates conflict with the intent, if not the requirements of R2 which still refers to a Responsible Entity "implementing" its policies. R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R2 also references a review without requiring any action as a result of the review, as discussed for R1. R4: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. Also, the words "and updated" in R4 should be removed. It is not clear how or why an initial delegation would be "updated" within 30 days of the initial delegation if no changes are made to the delegation. We suggest changing the wording to read "…updated within 30 calendar days of any change to the delegation…" CIP-004-5: R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R3: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. For clarity and to be consistent, a Part 3.6 analogous to CIP-004-5 R2 Part

2.2 should be added to CIP-004-5 Table R3. Currently R3 Parts have no clause to require that a PRA must be complete before granting access. Also R 3.5 should include a clause that it is subject to applicable law and collective bargaining unit agreements. We suggest adding Part 3.6 as the following: "Require completion of a PRA specified in Part 3.1 to 3.4 and in accordance with applicable law and collective bargaining unit agreements prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances." R3.1: It should clarify whose identity requires confirmation. R3.5: It does not meet the intent of 3.1 "Specified that identity confirmation is only required for each individual's initial assessment" as the part specifies 3.1 to be completed every 7 years according to "Parts 3.1 to 3.4 within the last seven years". We suggest rewording as follows: "Require completion of a criminal record check specified in Parts 3.2 to 3.4 for all individuals with authorized electronic or authorized unescorted physical access at least once every 7 calendar years." R4: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R 4.1: The phrase "based on need, as determined by the Responsible Entity" does not seem to add anything meaningful to the standard. The SDT should consider removing this phrase. R4.3: It is assuming an aspect (role-based privilege management) that has not been established nor defined in R4.1. We suggest either removing the phrase "and their specific associated privileges" from R4.3, or adding language regarding privilege levels in R4.1. R 5.1: Use of the phrase "termination action" could be interpreted to mean giving notice to terminate. Accordingly, for establishing the deadline by which a removal must be done, we suggest change the wording "termination of action" to "the effective date of the termination". R5.3: The word "action" should be deleted from the last portion of the requirement. We suggest wording "the next calendar day following the effective date of the termination". The phrase "and time" is unnecessary, given the reference to a calendar day rather than a twenty-four hour period. R5.4: Similarly, the word "action" should be deleted. CIP-006-5: R1: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R1.5: The words "of the unauthorized access" should be added to the end of the sentence. R1.7: "detected" should be added in front of "unauthorized access" in the fifth line. R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R2.2: It is unclear as to the time frame for this logging. Is the logging over a 24 hours period, during one business day, over the length of the visit (i.e. if someone is visiting for 3 days and coming and going each day)? We suggest putting a 12 hr timeline for last exit or "the last exit prior to leave the facility". CIP-007: R1: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R3: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R3.2: The word "identified" in the requirement is ambiguous and inconsistent with other malicious code phrases. We suggest changing to "detected". R4: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R4.5: To be consistent with other requirements, "15 days" should be changed to "15 calendar days". R5: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R5.4: The word 'known' is ambiguous - known to whom? Actual knowledge or 'should have known', 'could have known'? For clarity, we suggest changing "known default passwords" to "knowable default passwords". CIP-008-5: R1.2: This needs clarification. Does notification to ESISAC occur only if an identified Cyber Security incident is determined to be a Reportable Cyber Security incident? Also, it's not clear whether the one hour time line starts running at the identification of an identified Cyber Security incident or at the determination of that incident as reportable? Furthermore, there is no explanation of what a 'preliminary notice' is, is there a later final notice, etc. R2.1: "at least once every calendar year, not to exceed 15" is not consistent with the wording of other requirements. We suggest re-wording to read "at least once every 15 months". R3.1 and R3.2: The wording needs to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. CIP-009-5: R1.2: This talks about 'responders' with no description or definition of who fits this category. R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R2.1: The words 'between tests of the plan' are not needed. R3.1 and R3.2: The wording needs to be rearranged to read better - the words 'No later than 90 calendar days after' should be added at the start of the sentence and deleted from the end. CIP-010-5: R1: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R1.1: We suggest adding the words 'for each Cyber Asset' to the first line after configuration. R1.5.1: The comma after 'minimizes adverse effects' doesn't make sense, this should be 'and'. R2: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. R3.2: The requirement interchanges the words "assessment" and "test". It is recommended that one word be used consistently so there is no confusion as to what is intended. R3.4: It refers to an action plan that there has been no earlier requirement to prepare or develop. The requirement needs to specifically require that one be prepared. CIP-011-5: R1: Use of the phrase "implement in a manner that detects, assesses and corrects deficiencies" creates interpretational problems as explained in the global comments. Definitions: BES Cyber System Information: Regarding "not publicly available"; as currently worded, if information about the BES Cyber Systems, PACSs and EACMs is made publicly available, it is not BES Cyber System Information and would not require protection There is a potential that sensitive information could be made public

and outside the scope of the definition. Control Centre: Suggested wording to improve clarity: "One of more facilities that host operating personnel who monitor and control the Bulk Electric System (BES) in real-time. These operating personnel perform the reliability tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for transmission Facilities at two or more locations, or 4) a Generation Operator for generation Facilities at two or more locations. Control Centre facilities include associated data centers." CIP Exceptional Circumstance: This definition needs appropriate punctuation to separate the items in the list. The suggested definition is: "A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability." External Routable Connectivity: We suggest replacing "its" with "the BES Cyber System" for additional clarity. Interactive Remote Access: The sentence "Remote access can be initiated from: ... contractors and consultants." is guidance information, and restricts the definition to only applying to Responsible Entity Cyber Assets, employees, vendors, contractors, and consultants. By definition, this would exclude interactive remote access by anyone else (public, non-legitimate users) from scope. We suggest removing the last sentence and providing this information in a guidance document. Reportable Cyber Security Incident: Remove this definition and address in a standard(s). Reporting obligations should be in a standard, not in a definition. Physical Security Perimeter: Protected Cyber Asset is missing from this PSP definition, otherwise CIP-006-5 won't apply to PCA. Implementation Plan: 1. Under the heading "Proposed Effective Date for Version 5…", there is a statement that "Notwithstanding any order to the contrary, CIP 002-4 through CIP-009-4 do not become effective, and CIP-002-3 through CIP-009-3 remain in effect and are not retired until the effective date of the Version 5 CIP Cyber Security Standards under this Implementation Plan." This statement should either be stricken or at least confined to FERC orders. NERC does not have the legal authority to usurp regulatory orders, or other government approvals in Canadian jurisdictions, through publishing an implementation plan. The only possible exception is where the regulator itself (such as FERC) approves the implementation plan through issuing an order, usurping its previous orders. Since Canadian jurisdictions do not have regulators that issue orders approving implementation plans, this cannot be accomplished in Canada through an implementation plan. 2. In the section regarding periodic performance of certain requirements, NERC proposes to impose certain requirements before or on the effective date of a standard. Again, this goes beyond NERC's legal authority. If a government or regulatory body determines an effective date for a standard, NERC cannot compel performance prior to that effective date. With respect to the imposition of certain periodic requirements on the effective date of a standard as well as periodically, the specific standard must be revised to include an additional requirement to perform that requirement on the effective date. An Implementation Plan is not a standard.

Individual

Andrew Z. Pusztai

American Transmission Company

Individual

Silvia Mitchell

NextEra Enregy

The drafting team has done an excellent job of improving Version 5 (V5) while also addressing many of FERC's Order 706 suggestions in the face of divergent industry views and points of emphasis. NextEra Energy, Inc. (NextEra) is voting Affirmative on CIP-002-5, CIP-003-5, CIP-005-5, CIP-008-5, CIP-011-5, and Definitions, while voting to Abstain with comments with respect to CIP-004-5, CIP-006-5, CIP-007-5, CIP-009-5, CIP-010-5, and the Implementation Plan. NextEra voters will reconsider Abstain positions on these 6 items (either for another successive ballot or upon a recirculation ballot) if: (a) the zero defect fix language ("in a manner that identifies, assesses, and corrects deficiencies" (the IAC Language)), which is applicable to 66 different requirements in draft 3 of V5, is supplemented, revised and/or better clarified; and (b) the Implementation Plan is improved, both as further described below. With respect to (a), the draft RSAW for CIP-006-5 is a welcome gesture and a step in the right direction, but it is flawed, insufficient, and does not change the fact that the IAC Language used in the standard is ambiguous and untested. The IAC Language does not explicitly address the issue of whether and, if so, when internally identified and corrected deficiencies constitute violations of the standard's requirements. The proposed RSAW language regarding "deficiencies" and "self-reporting" does not adequately resolve this ambiguity; if anything, it further muddies the water. It is unclear to NextEra whether any amount of verbiage in an RSAW can cure ambiguity flowing from the standard language itself. With respect to the words chosen, by prefacing the IAC Language with the phrase "in a manner that," which is itself prefaced by the words "shall implement," the requirement has become more, not less, rhetorically prescriptive. This is a step in the wrong direction, as NextEra and others were hoping the language chosen would not be in the form of an additional command, but would simply give their cyber security staff the freedom they need to develop robust internal correction programs, especially for high-volume, periodic activities. For companies like NextEra that operate in multiple NERC regions, the prospect of inconsistent and un-coordinated compliance evaluations raises serious concerns about whether the IAC Language could be applied and utilized in different ways across the country. To prevent this vacuum of ambiguity from being filled with negative unintended consequences, NERC must find an expeditious way to modify, clarify, or at least standardize the interpretation the IAC Language. One option is the insertion of an addendum to V5 between the

putative approval of draft 3 on October 10, 2012 and the final recirculation ballot that must be held before the new standard is ripe enough to forward on to the NERC BOT. Such an addendum could be narrowly focused on soliciting stakeholder input and consensus regarding ways to modify, interpret and/or clarify the IAC Language in a way that makes sense for all stakeholders. NextEra's specific suggestion for improving the IAC Language is to strike the entire phrase, then insert a new, longer sentence fragment at the end of the current sentence: "[Each Responsible Entity shall implement one or more documented physical security plans that collectively include all of the applicable items in CIP-006-5 Table R1 – Physical Security Plan], provided that internally identified deficiencies that are documented, assessed, and corrected if necessary as determined by the Responsible Entity, shall not constitute per se violations of this R1." The generic use of the legal phrase "per se" is a potentially promising way of addressing the violation issue directly in the standard itself. With more explicit, robust language in the standard, it would be easier for industry and NERC to facilitate a broader shift to risk-based auditing based on internal controls. To that end, in addition to changes to the standard itself, NextEra supports the following RSAW language for CIP standards with IAC Language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." Also please consider this language for the RSAWs: "R1 Absent a possible violation that resulted in (or could have resulted in) a significant risk to the Bulk Electric System, no violation of R1 and its subrequirements shall be found, provided that the Responsible Entity has implemented a process for identifying, assessing, and correcting deficiencies with adherence to the items specified in Requirement R1." Moving to a new topic, item (b) above, NextEra has voted to Abstain with respect to the Implementation Plan for the following reasons. The Implementation Plan fails to specifically say that NERC will ask FERC to suspend the April 1, 2014 effective date for Version 4 (V4) when it submits V5 for FERC approval prior to March 31, 2012. Without suspension of the V4 effective date, NextEra is among those that will be forced to follow a parallel and costly approach to sustaining compliance to Version 3, implementing V4 by April 1, 2014 for newly identified Critical Assets, and implementing V5, which eliminates the term Critical Assets, for its presumed effective date of July 1, 2015. The current plan is a recipe for costly stranded costs that do not improve reliability. The drafting team can and should address this important problem in the Implementation Plan. Alternatively, NERC can and should ask FERC to move quickly to approve V5 once it is submitted for approval, or at least move quickly to suspend the effectiveness of V4 pending FERC's review of V5. In addition, NextEra believes the line between planned and unplanned changes is not always easy to maintain and there may be times it is appropriate to let a planned change become fully compliant at some time after the cyber system is commissioned. Similarly, after initial implementation of V5, there is an inadequate amount of time allotted for the implementation of the V5 Standards for BES Cyber Systems that go from the "Low" to "Medium" or "High" impact categorization based on unplanned enhancements and improvements to facilities. Responsible entities should be given 18-24 months, not merely 12 months, to comply, as many of the compliance activities can only be accomplished during planned outages at generation facilities. NextEra also finds the section on Initial Performance of Certain Periodic Requirements to be confusing and unnecessary and urges the drafting team to strike it or qualify these timing recommendations as proposed guidance, rather than a mandatory directive for all Responsible Entities to follow. If the section must remain, NextEra suggests it allow for an alternative timing option for periodic requirements that pegs all of the V5 requirements to the Effective Date and lets the Responsible Entity begin meeting the periodic items as they arise naturally in accordance with the CIP standards' periodic requirements.
NextEra thanks the drafting team for its hard work and the improvements it has made to Version 5.
Individual
Patrick Brown
Essential Power, LLC
1. Definitions - all standards Control Center: We believe that control centers require an appropriate level of protection for the bulk electric system and its components as identified in the FERC Orders 761 & 706. We also understand the expectation of "comprehensive protection of all control centers and control systems as NERC works to comply with the requirements of O-706". However, we urge the Drafting Team to establish appropriate levels of impact (High, Medium & Low) through the application of a 1500 MW generation and 1000 MVAr bright-line thresholds. This would be applied to Transmission Operator Control Centers where their impact would be minimal and would be consistent with the application of the generation and balancing authority bright lines as found in the Medium impact section of CIP-002-5 Attachment 1. Associated data centers: 'data centers' is not a defined term. The SDT should define the term, or add a statement that entities must define the term for themselves. 2. CIP-003 Background & all standards where the language is used Zero Defect/Internal Controls language: Although we fully support the implementation of Internal Controls as part of NERC's Reliability Based Standards initiative, it is unclear how this will be applied in practice. For those of us registered in multiple Regions, there is some concern regarding consistent application of this concept.
Individual
Tom Washburn
FMPP
Group

Wisconsin Electric Power Company NCR00951

Steve Karolek

CIP-002-5 "bright line criteria" #2.3, which states "2.3 Each Generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year" presents uncertainty and challenge to the industry. Unlike criteria 2.1, 2.2, 2.4, 2.5, 2.10, 2.11 and 2.13, all of which include specific measurable thresholds, criteria 2.3 relies on notification from a Registered Entity who is not subject to the CIP standards (none of the CIP standards are applicable to the PCs and TPs) related to a theoretically possible cascading islanding of firm load in a planning study of possible future conditions. The standard does not include any requirements specifying how we would document that we have or haven't received such notice or worked with our PCs and TPs to determine if they have run any such studies. The standard does not include any requirements relating to the inputs and assumptions of any such studies, and the standard does not include any indication of what amount of firm load islanded represents an Adverse Reliability Impact. The criteria would be enhanced significantly with the inclusion of an applicability threshold of at least 300mw (analogous to the firm load control threshold in criteria 2.10 related to dropping firm load under UFLS or UVLS controls) and the standard would be enhanced with the addition of requirements providing direction on what type of compliance artifacts would be appropriate to demonstrate compliance with the notification aspects of the criteria. CIP-002-5 through CIP-009-5, CIP-010-1 and CIP-011-1 all contain boilerplate applicability language in section 4.2.2 which could be read and interpreted so as to exclude certain Registered Entities including RC, BA, LSA, IA and possibly others, from mandatory compliance to the NERC CIP standards requirements due to their not having any "BES Facilities". Since section 4.2.2 does not appear to serve any specific purpose, our recommendation is to remove it from all of the draft CIP standards in order to eliminate the potential confusion and misinterpretation.

Individual

Don Jones Jones

Texas Reliability Entity

We are voting "no" on proposed standard CIP-010-1, because in Requirement 3 it is not clear regarding what comprises a complete and documented vulnerability assessment. This important requirement is subject to broad interpretation and too much subjective judgment. We recognize the attached guidelines provide elements that entities are "strongly encouraged" to include in a vulnerability assessment, but without mandatory elements or a clear definition we feel that this requirement may allow reliability gaps to exist.

The identify, assess, and correct (IAC) approach used in these standards does not require any interim reporting of deficiencies, or their frequency and severity. As the Compliance Enforcement Authority, we are concerned that with no timely information about deficiencies that occur we are not able to monitor an entity's compliance with its own IAC process and the effectiveness of that process. For example, repeated deficiencies may indicate that the entity's corrective actions are not effective, or that other mitigating measures need to be taken. We suggest adding a reporting process to provide information about an entity's use of its IAC process (including identified deficiencies) between formal audits.

Individual

John Souza

Turlock Irrigation District

Individual

Rich Salgo

NV Energy

I will be voting affirmative for both of the Standards for which problems are noted below; however, I believe these two issues bear addressing by the SDT. CIP-002-5 Attachment 1 section 2.4: In this section, medium impact is assigned to Transmission Facilities operated at 500kV or higher. In the previous comment period, NV Energy noted that we believe an exclusion is warranted for distribution stations that are situated at the receiving end of a radial 500kV line. Specific instances exist of 500/69kV stations whose only purpose is to provide distribution service. In light of the SDT's clarification within 2.4 to specifically exclude collector buses for generation plants, we believe it is even more compelling that such an exclusion be given for receiving stations having 500kV or higher source voltages. Our review of the SDT's consideration of comments for the 2nd posting revealed no mention of this prior comment, while our understanding is that all negative comments received were owed a consideration through the Standards Development Process. CIP-004-5 R3.1 Under the parent requirement R3, the entity is to implement a risk assessment program to attain AND retain authorized access. Identity confirmation is one of the program elements, and it is prescribed in Part 3.1. However, the Change Rationale section for Part 3.1 states that it was specified that ID confirmation is only required for each individual's initial assessment. This change rationale would therefore indicate that ID confirmation is not required for retention of access, but only for the attainment of initial access. The SDT should address this inconistency and clearly indicate whether ID confirmation is required at the initial attainment of access, or for both attainment and retention of access.

Individual

Michael Mertz

PNM Resources

Minor recommended edits: CIP-008: Recommend changing 1 hour reporting window to 24 hours to align with EOP-004 CIP-010: R1.4.2 can be interpreted to mean "in production", clarification recommended

Individual

Annette Johnston

MidAmerican Energy Company

MidAmerican Energy Company voted affirmative for all ballots. Specific, important items we do not support are detailed in question 2. Lack of clarity and/or transparency are the specific reasons for not supporting these items. Changes to clarify these items for a recirculation ballot to achieve the draft 3 intent are possible without being significant.

The following comments improve transparency and/or clarity of intent without being significant changes. (1) Zero defect: Add the following to requirements that include the "in a manner that" language: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing the requirement." (2) High water marking: Per the Guidelines and Technical Basis for CIP-005-5 R1, all of the Cyber Assets and systems, even other BES Cyber Systems of lesser impact, within the ESP will be elevated to the level of the highest impact BES Cyber System present in the ESP. This vital concept should be included in section 5 Background of every standard, not just in CIP-005 guidance. (3) ERC: This concept is included in section 5 Background of standards, "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." This vital concept should be included in the definition of External Routable Connectivity and include "ERC" as an acronym in the glossary. (4) 004 and 007 accesses: Issues with lack of understanding and inconsistent implementation have been identified for authorized access list and specific rights reviews in versions 1-3 CIP-004 R4, CIP-003 R5 and CIP-007 R5. We are concerned that CIP-004-5 R4.2 and R4.3 quarterly and annual verifications are predicated on some generalizations and/or assumptions that are not complete and will not sufficiently resolve the existing issues. And as drafted, an entity has to infer or assume from CIP-004-5 R4.4 that storage location accesses are not included in R4.2 or R4.3. Additionally, CIP-007-5 R5.2 and R5.3 will exacerbate the issues in CIP-004 R4.2 and R4.3. CIP-007-5 R5.2 and R5.3 can be achieved most effectively by consolidating them in CIP-004-5 R4 to eliminate redundancy, double jeopardy and improve clarity. Access authorizations and provisioning warrant further clarity in the recirculation ballot because they require significant resources, involve extensive complex data and are among the most currently violated requirements. We respectfully request reconsideration of the issues and the constructive solutions we offered to the drafting subteam for draft 3.

Individual

Steven Powell

Trans Bay Cable LLC

Comments with negative vote to CIP-002-v5 The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES. The stated Purpose of the Standard CIP-002-5 as proposed is: To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. TBC comments that it is not clear to our organization that certain provisions within this proposed Standard stand up to the test of commensurate with the adverse impact that loss, compromise, or misuse could have on the reliable operation of the BES. Using the stated Purpose statement as the measure during our final review of the proposed Standard and the accompanying definition of Control Center, TBC was not able to support an affirmative vote as outlined below: Criterion 2.5: It does not appear to TBC that the SDT has considered adequately the nuances of Direct Current facilities (at least those owned and/or operated by entities that are not part of a much larger integrated AC network that fall under any new "Control Center" definition by default) and the design and capabilities of such facilities when applying the attributes of the NERC "Integrated Risk Assessment Approach – Refinement to Severity Index" to DC facilities. The terminal voltage of a DC facility is not the driving factor of the severity of the risk to the Bulk Electric System rather it is the overall capability of the fully controllable system and the risk of compromise to that level. It is the opinion of TBC that a better approach to measure risk to the BES for DC facilities should be in parallel with what the SDT proposes for generators in criteria 2.11 and 2.13; Reasoning: DC systems are modeled almost exclusively in wide area models as a load at the source, and a source (generator) at the delivery point. For example a controller of two geographically and electrically diverse DC facilities with 345KV terminals capable of 700Mw each is to be scored to a weighted valued of 5200 under the proposal and therefore receive a Medium Impact Rating (if operated from a single control room or Control Center), compared to an owner/operator of two separate generators, rated at 700Mw each, and again in geographically and electrically diverse areas to be ranked at Low Impact. Or alternatively, a superior approach for DC facilities in which it is required to apply NERC Planning Category C or D

risk assessment to these facilities in aggregate; Reasoning: A single DC facility, if compromised is currently a NERC Category B contingency and therefore not a risk to the BES or IROL. If multiple DC facilities have common control points whether via control room, or "Control Center" the study of the area impact of the compromise of all DC facilities under the common control point is technically feasible and should be allowed by Standard rather than the proposed and inferior "Integrated Risk Assessment Approach" used as a proxy for the importance of AC facilities. Proposed Definition of "Control Center" In addition to our concern with the approach used in criteria 2.5, during our review and decision process regarding a positive or negative vote for CIP-002 v5 there were two items that we were not able to find consensus of meaning or any interpretation on to support a positive vote: • TBC needs clarification of what is meant by the term "associated data centers" as used in the proposed definition. • TBC needs clarification of what is meant by the term "locations" as used in the proposed definition.
Proposed Definition of "Control Center" In addition to our concern with the approach used in criteria 2.5, during our review and decision process regarding a positive or negative vote for CIP-002 v5 there were two items that we were not able to find consensus of meaning or any interpretation on to support a positive vote: • TBC needs clarification of what is meant by the term "associated data centers" as used in the proposed definition. • TBC needs clarification of what is meant by the term "locations" as used in the proposed definition.
Individual
Guy Andrews
Georgia System Operations Corporation
no comment
GSOC appreciates the CIP V5 SDT time and effort on addressing industry's issues with the CIP standards. GSOC is strongly supports the following NRECA comment: Internal Control Language and VRFs/VSLs – The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. GSOC appreciates the SDT's efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, GSOC is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exist today. GSOC supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.
Individual
Brian Evans-Mongeon
Utility Services
Utility Services believes that the applicability section of the standard creates instances of where the intended CIP applicability is not consistent between functional registrations. In Section 4.1.2.4, Cranking Paths owned by Distribution Providers are applicable to the CIP standards. However, under Section 4.2.2, only BES Facilities are applicable to Transmission Owners and Transmission Operators. Since Cranking Paths are not necessarily BES Facilities by either today's regional definitions or the proposed BES Definition, the applicability language in the standard would only make Cranking Paths owned by Distribution Providers subject to the CIP standards. Cranking Paths owned or operated by TOs or TOPs would not applicable to the standard unless they are part of the BES. Therefore, Utility Services asks the SDT to consider changing the applicability language in Section 4.2.1.4 to from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching..."
Individual
William O. Thompson
NIPSCO
Individual
David Gordon
Massachusetts Municipal Wholesale Electric Company
(Comment 1) MMWEC supports the comments submitted by NPCC. (Comment 2) Section 4.1.2.4 includes ownership of a Cranking Path as a criterion for applicability of the CIP standards for Distribution Providers. However, Transmission Owners may own Cranking Paths that are less than 100 kv and not necessarily part of the

BES. As written, the CIP standards would not apply to those non-BES Cranking Paths owned by Functional Entities other than DPs because section 4.2.2 specifies "All BES Facilities" for applicability to other Functional Entities. 4.1.2.4 should be changed from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching..." Each region may identify Cranking Paths that are critical to the restoration plan and may use the BES exception process to classify those Cranking Paths as BES Facilities. CIP standards should apply to Cranking Path cyber systems that are part of the BES and that are owned or operated by any Functional Entity. Cranking Path equipment that Regional Entities do not classify as part of the BES would be exempt from the CIP standards, unless the equipment is included due to other criteria. This will be consistent with the concept of protecting BES Cyber Systems, provide consistency of applicability across all Functional Entities regarding Cranking Paths and clarify which equipment owned by DPs is subject to CIP standards.

Group

National Rural Electric Cooperative Association (NRECA)

Barry Lawson

NRECA very much appreciates the efforts of the CIP V5 SDT on addressing industry's issues with the CIP V5 draft standards. Many issues have been satisfactorily addressed; however, NRECA remains concerned with the criteria in CIP-002-5, Attachment 1, as it relates to TOPs. We believe it is appropriate for TOPs to be treated similarly to BAs and GOPs as far as how they are ranked in the High, Medium and Low Impact Rating categories. BAs and GOPs are ranked in all three categories based on specific criteria – TOPs should receive similar treatment. NRECA strongly recommends the following changes to CIP-002-5 Attachment 1 to ensure the fair and equitable treatment of TOPs that only control facilities operated at less than 200 kV (new language is in ALL CAPs): 1. Criteria 1.3 does not require any changes. 2. Criteria 2.12 should be revised to state "Each Control Center or backup Control Center used to perform the functional obligations of the Transmission Operator not included in High Impact Rating (H), above, AND THAT CONTROLS TRANSMISSION FACILITIES OPERATED AT 200 KV AND ABOVE." 3. A new criteria should be added to the Low Impact Rating (L) section to state "EACH CONTROL CENTER OR BACKUP CONTROL CENTER USED TO PERFORM THE FUNCTIONAL OBLIGATIONS OF THE TRANSMISSION OPERATOR NOT INCLUDED IN HIGH IMPACT RATING (H) OR MEDIUM IMPACT RATING (M), AND THAT ONLY CONTROLS TRANSMISSION FACILITIES OPERATED BELOW 200 KV."

Internal Control Language and VRFs/VSLs – The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. NRECA appreciates the SDT's efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, NRECA is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exists today. NRECA supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.

Individual

Linda Campbell

FRCC

Identify, Assess, and Correct Deficiencies The language of "each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies." is somewhat problematic. This language does not outline the timeframe an entity has between identifying and correcting a deficiency. Can an entity take 24 months to correct a deficiency? Probably not, based on auditor judgment. However, this type of language leaves a lot to be interpreted on both the RE and the entity sides. Additionally, there is no language that addresses the magnitude of a deficiency. For example, if an entity finds that they did not deploy a method to deter, detect, or prevent malicious code on all 15 of its firewalls (CIP-007-5 R3) for two years but then determines right before an audit that they missed this requirement, does this qualify for "identify, assess, and correct deficiencies?" What if they identified 5 of those 15 as not being corrected? Is there a breaking point in terms of quantity before a deficiency becomes a possible violation or a Self Report is required? As written, the requirement does not set ANY time limit for mitigating "the threat of identified malicious code." An entity that decided the mitigation will have to wait until an outage 2 years out will still be in compliance but the threat to the BPS is still there. Ports and Services CIP-007-5, R1.1: "If a device has no provision for disabling or restricting logical ports on the device, then those ports that are open are deemed needed." The requirement does not provide any provisions for limiting access to those ports or

services that cannot be disabled. The requirement's measures ask for host-based protective measures. For those devices that are not capable of providing localized protective measures, such as relays, there is a question as to how this requirement would be met. Previously, when a port or service could not be disabled, a TFE would require mitigation of the potential vulnerability. Under CIP-007-5, if the entity leaves these ports and services open they are in compliance but there is a question of whether the vulnerability of the device still remains. Summary To better protect the BES, there is an advantage to moving towards V5 and bypassing V4. NERC's Risk Based approach is also the way the rest of other industries tackle security management. Entities will benefit more from an audit that is risk based because it provides for a tailored approach and allow fine-tuning to take place. Like V3, the V5 objective is to apply security in layers (known by other industries as defense-in-depth approach) so that if one area is compromised or circumvented, at least another measure continues to provide protection. Is a layered approach a 100% fool proof? No, take for example CIP-005 ; it implements a series of security controls, however, this does not mean that by passing the audit the entity is not vulnerable by the way it has implemented the controls. As stated above there still remains wording in the standards that should be clearly defined to reduce number of interpretations and increase consistency across regions. We believe it is in these areas where NERC and the SDT should make sure they reduce or eliminate these wording interpretation challenges. CIP 5 is a much more robust and complex set of standards that will require more compliance and auditing resources for both the ERO and the entity. I will vote for approval as it does a much more thorough job than the present standards in protecting the Bulk Power System.

Individual

Oscar Herrera

Los Angeles Department of Water and Power

CIP-004 R5.2 – The time limits for revoking access upon terminations and transfers being proposed for the next calendar day present extreme challenges. More time needs to be given. The next business day for terminations and 3 business days for transfers will make these processes manageable. The following additional requirements may be onerous compared to the benefit received: •Required IDS/IPS for firewalls •Encryption between links •Multi-factor authentication for remote access AND encryption CIP-006 Part 1.6 – A responsible entity needs to monitor each PACS system for unauthorized physical access to a PACS. However, there is no requirement that the PACS be contained within a PSP. Therefore, how does one control physical access to the PACS? CIP-006 Part 1.7 requires to issue an alarm or alert in response to detected unauthorized physical access to a PACS to personnel identified in the BES Cyber Security Incident Response Plan within 15 minutes of the unauthorized physical access. However, CIP-008 does not include the PACS in the Cyber Security Incident Response Plan. CIP-006 Part 1.3 requires two or more different physical access controls… which is overkill. 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 Center typically already have stringent physical security controls and monitoring CIP-006 Part 2.2 would require manual or automated logging of entry and exit from the physical security perimeter. The requirement for egress has not been explicitly defined as a requirement. Preference is for ingress logging only. An egress requirement has been alluded to in the requirement. Access controls for egress presents a number of safety issues and concerns. CIP-007 Part 4.2 states that an entity needs to generate alerts for security events that the entity determines necessary. An entity defined security events seems like a questionable and subjective requirement. Further, although not explicitly stated in the standard, the guidelines and technical basis attachment suggests that R4.2 be in real-time and this may be an issue. CIP-009 Part 2.1 states that the entity is to test the recovery plan(s) every calendar year, not to exceed 15 months. Part 2.3 seems to be a facsimile of 2.1, yet adds a longer timeframe for compliance. We need clarification on the timeframes, as there may be overlap between the two activities. Furthermore, there needs to be clarification or additional guidance for the types of operational exercises the drafting team is requesting entities to perform per Part 2.3. CIP-010 Part 3.3 states that prior to adding a new Cyber Asset to a BES Cyber System, the entity is to perform an active vulnerability assessment of the cyber asset. It is problematic to perform an active vulnerability assessment prior to installing a new Cyber Asset. Furthermore, the term "Active vulnerability assessment" is not defined. Under the assumption that an "active vulnerability assessment" is the actual performance of an entities vulnerability assessment program, there are sufficient controls in place that would deem an "active vulnerability assessment" unnecessary, such as change management procedures. Therefore, we request that Part 3.3 be removed.

Individual

Thomas A Foreman

Lower Colorado River Authority

• In CIP005-5, R1.5, we propose the following: "Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. ESP-to-ESP communications within a discrete BES Cyber System shall be excluded." As an example, the communication links between a primary transmission control center and its backup control center shall be excluded. • For clarification, in CIP 007-5, R4.4,

in the requirements column of the table, the draft language indicates a need to review logs to "identify undetected Cyber Security Incidents." Is this intended to be "identify detected Cyber Security Incidents?"

Individual

Kayleigh Wilkerson

Lincoln Electric System

Although supportive of the drafting team's efforts and responsiveness in addressing our previous concerns, LES requests that the following concerns be considered prior to approval. CIP-002-5 R1: Recommend the 6 asset categories included as part of R1 be removed and the drafting team instead reference Attachment 1, if needed, to ensure consistency in language as well as prevent unnecessary duplication. CIP-002-5 Attachment 1-1.3: For Attachment 1-1.3 "Transmission Operator Control Centers", LES believes additional thresholds should be included to better delineate High Impact from Medium to Low Impact Control Centers. Potential thresholds to include are as follows. (1.3). Each Control Center or Backup Control Center used to perform the functional obligations of the Transmission Operator for 4 or more of the assets that meet criterion 2.2, 2.4, 2.5, or 2.10; or for any asset that meets criterion 2.6, 2.7, 2.8, or 2.9. (2.12). Each Control Center or Backup Control Center used to perform the functional obligations of the Transmission Operator for one or more of the assets that meet criterion 2.2, 2. 4, 2.5, or 2.10. CIP-002-5 Attachment 1-2.5: The total of the aggregated weighted values calculated should be divided by 2 to get a better representation of the impact to the BES for the loss of through flows. The number of lines should at least be increased to 4 or more to have at least a 2600 (MVA) aggregated weighted value impact to the BES. This would be more in line with the BA and GO bright-line thresholds. With only 3 lines at 300-499KV, an entity can only have a max through flow of 1300. When you only have 4 lines, the through flow increases to 2600 MVA (2 lines with flows in and 2 lines with flows out) Suggestion: Either take the Weight value per line and divide them in half: 200 kV to 299 kV 350 300 kV to 499 kV 650 Or as an alternate: 2.5. Transmission Facilities that are operating between 200 kV and 499 kV at a single station or substation that is connected to 4 or more other Transmission stations or substations and has "aggregate weighted values" exceeding 3000 according to the table below….." CIP-005-5 Background Section: To ensure consistency between the standard and the list of "Definitions of Terms Used in Version 5 CIP Cyber Security Standards", LES asks that the drafting team update the CIP-005-5 Background section to reflect the same definition as used in the list of definitions of terms. CIP-007-5 R2.1: The patch management process for substation or plant control systems could include security patches for Cyber Assets such as panel meters, relays, controllers, PLC's, and other electronic devices that are part of the BES Cyber System and do not have network connectivity. Recommend R2.1 and R2.2 be rewritten as follows to only include those assets that are connected to a network. (R2.1). For all Cyber Assets connected to a network via a routable protocol, the Responsible Entity has a patch management process for tracking, evaluating, and installing… (R2.2). For all Cyber Assets connected to a network via a routable protocol, at least once every 35 calendar days, evaluate security patches… CIP-007-5 R4.1: As currently written, R4.1 would necessitate the logging at every Cyber Asset that is capable when there is not a network at the BES Cyber System. As such, every Cyber Asset would be considered an access point. To prevent undue burden on registered entities, recommend R4.1 be rewritten as follows: (R4.1). For BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol, log events at the BES Cyber System Level… CIP-007-5 R4.3: Recommend that the log retention requirements be included as part of the data retention portion of the standard rather than as part of the requirement. CIP-008-5 R1.3: Recommend removing R1.3 and leaving it to the registered entity's discretion as to what information is to be included within the response plan(s). By creating an all-inclusive list of roles and responsibilities, an auditor could potentially question why certain roles or responsibilities were left out of the response plan or why particular individuals were granted certain roles or responsibilities (i.e. qualifications, experience…). If the entity has a Response Plan, that should be sufficient without needing an additional requirement for what should be included in the plan. CIP-008-5 R2.1: Recommend R2.1 be written to state that one Cyber Security Incident response plan would be sufficient for High Impact and Medium Impact BES Cyber Systems. Suggested wording includes the following: (R2.1). Test at least one High Impact and Medium Impact BES Cyber Security Incident response plan(s) at least once every calendar year, not to exceed 15 months… CIP-008-5 R2.3: This requirement should be moved to the data retention portion of the standard. CIP-008-5 R3.2: As stated in R1.3, LES believes defining and listing individual roles and responsibilities as part of the Cyber Security Incident response plan(s) is needless administrative work and should be left to the discretion of the registered entity. If R3.2 is to be retained, recommend that at a minimum it be rewritten to remove R3.2.2 as well as the first paragraph and simply state the following: (R3.2). After an update to the Cyber Security Incident response plan(s) occurs, notify affected person(s) or group(s), not to exceed 60 calendar days. CIP-009-5 R1.2: Similar to comments made for CIP-008-5, LES believes R1.2 is an unnecessary administrative requirement that does not allow registered entities the flexibility to adapt and change their plan(s). If not removed, recommend that at a minimum, R1.2 be rewritten to state that an entity need only have responders in the event that the recovery plan(s) were to be activated. CIP-010-1 R1.1-R1.4: The requirements should only apply to networked Cyber Assets, otherwise a very labor intensive process will be needed for collecting and reviewing baseline configurations for numerous stand-alone electronic devices used in the BES Cyber Systems. Suggest adding the following statement at the beginning of each requirement: "For BES Cyber Systems that have Cyber Assets connected to a network via a routable protocol,…". CIP-010-1 R3.4: Requirements 3.2 and 3.3 do not apply to Medium Impact BES Cyber Systems, however, R3.4 requires the entity to document the results of Parts 3.1, 3.2, and 3.3 for both High and Medium Impact BES Cyber Systems. To

ensure consistency with the individual Parts, recommend Part 3.4 Applicable Systems be modified as follows: - High Impact BES Cyber Systems (as it applies to Parts 3.2 and 3.3) and their associated:… -Medium Impact BES Cyber Systems (as it applies to Part 3.1) and their associated:…

Individual

Heather Laws

Portland General Electric Co.

n/a

DRAFT 3 - There are still several places where the details need to be cleaned up and consistent. See CIP-004 for the "and/or" and granting vs. provisioning inconsistancies in the rational, guidelines and even in the requirment and measures sections. Also very concerned that no where in CIP-006 does it say that you have to define a PSP. Is it just assumed? I don't think we can just assume.

Individual

Bob Thomas

Illinois Municipal Electric Agency

Individual

David Revill

Georgia Transmission Corporation

GTC appreciates the CIP V5 SDT's time and effort addressing industry's issues with the CIP standards. GTC supports the following NRECA comment: Internal Control Language and VRFs/VSLs – The inclusion of the language "Each Responsible Entity shall implement, in a manner that identifies, assesses, and corrects deficiencies, . . .", commonly referred to as internal control language, is a significant change to the CIP V5 standards that was added very late in the development process of these standards. GSOC appreciates the SDT's efforts to address zero-defect language in the standards and to propose a potential alternative. The concept of permitting a registered entity to address deficiencies with corrective actions without them becoming violations is one that many can support. However, adding this internal control language so late in the drafting of the CIP V5 standards raises significant uncertainty and confusion. Also of concern is the fact that the currently proposed VRFs and VSLs do not clarify what a violation looks like under the new approach. The language is also unclear on what is not considered a violation. The primary concern and source of confusion is how such a programmatic approach will be audited. In supporting the CIP V5 standard proposals, GSOC is taking a leap of faith that NERC leadership and staff will work carefully and collaboratively with industry to clarify the compliance component of this language to ensure that it addresses the targeted intent and does not create any additional compliance burdens to the current substantive compliance burden that exist today. GSOC supports the internal controls concept, but significant work is needed to help industry to understand and support the compliance obligations and enforcement measures around this concept. This work needs to be completed well before the CIP V5 standards become effective and auditing begins on the new provisions – assuming appropriate regulatory approvals are secured.

Individual

John Allen

City Utilities of Springfield, MO

City Utilities appreciates the changes made in the latest draft of CIP-002-5 to allow some BA Control Centers to be designated as Low Impact. However, we are continuing to vote negative on the Standard and ask the SDT to keep working to develop a bright-line for small TOP Control Centers that will allow them to properly be identified as Low Impact. If the next draft contains proper consideration for small TOPs, then we will vote affirmative in the next ballot period. City Utilities has worked with APPA and TAPS to provide options for the SDT to consider. City Utilities supports the comments submitted by these organizations.

Group

PacifiCorp

Ryan Millard

PacifiCorp is concerned: (1) with how CIP-002, Attachment 1 2.6 and 2.9, should be implemented within WECC due to the fact that IROLs have yet to be clearly defined by the RC and, once defined, may be short term in nature, making it very difficult to implement compliant CIPS programs that proactively identify all necessary BES Cyber Systems; (2) that the requirement for Responsible Entities to utilize two or more physical access controls, under CIP-006 R1.3, will be an increased expense and administrative burden for entities with only a minimal benefit to physical security; (3) that the short period between the effectiveness of approved Version 4 and advent of Version 5 requires fully revised CIPS compliance programs, making the back-to-back implementation of the different standard structures expensive and counter-productive. PacifiCorp recommends that NERC support an implementation approach whereby if Version 5 is approved, it would supersede Version 4 in its entirety. PacifiCorp

also recommends that the drafting team add an exclusionary concept to the definition of "External Routable Connectivity" so that Cyber Assets within a BES Cyber System that cannot be directly accessed through External Routable Connectivity would be expressly excluded from the definition, and add "ERC" as a defined acronym.
Individual
Linda Jacobson-Quinn
Farmington Electric Utility System
Individual
Southern California Edison Company
NERC Compliance Program
CIP 002 Attachment A Section 2.1 Please define "Commissioned Generation" Section 2.9 Please clarify how Attachment A Section 2.9 impacts entities with no IROLS? Attachment A Please clarify that since the term "associated data centers" has been removed from Attachment 1 in Draft 3, it should also be removed from the Guidelines and Technical Basis section: CIP 004 R5.2 Requirements Please clarify how to record the date that the entity determines that the individual no longer requires retention of access? CIP 007 Effective Dates …the effective date of the order providing applicable regulatory approval, and Requirement 5.2 shall become effective 12 months later, as to provide entities more time to identify and inventory all enabled default or other generic account types. R3.2 Applicability Revise to apply to Medium Impact assets with external routable protocol: "Medium Impact BES Cyber Systems with external routable protocol and their associated" R4.1 Requirements Revise to include the sentence from the guidance: …that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability):the Responsible Entity determines which computer generated events are necessary to log, provide alerts and monitor for their particular BES Cyber System environment.
Individual
Joe O'Brien
NIPSCO
NIPSCO does not support the following definitions as proposed: a. BES Cyber Asset – The definition should reference "the items in Attachment 1" instead of "Facilities, systems, or equipment," because "Facilities, systems, or equipment" is subjective and lends itself to differing interpretations, and Attachment 1 provides greater clarity and guidance on the criteria to define BES Cyber Assets. b. CIP Senior Manager – NIPSCO recommends modifying this definition to provide the clarification requested under RFI Project 2012-INT-06. Modify the definition to: "A single senior management official of a registered entity with overall authority and responsibility for leading and managing implementation of and continuing adherence to the requirements within the NERC CIP Standards, CIP-002 through CIP-011." c. Cyber Asset – The proposed definition could be interpreted to require utilities to demonstrate consideration of – in addition to hardware – all software and data on each programmable electronic device, which would be impracticable and overly burdensome. NIPSCO recommends changing the definition to "Programmable electronic device." d. BES Cyber System Information – The definition should include only BES Cyber System Information that is under the control of the responsible entity. e. Electronic Access Control or Monitoring Systems ("EACMS") – The definition should not reference "Intermediate Device" because Intermediate Device is a uniquely defined term. f. Electronic Access Point ("EAP") – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: "A Cyber Asset interface to an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter." g. Electronic Security Perimeter ("ESP") – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: "The logical border to a network in which BES Cyber Systems are connected using a routable protocol." h. Intermediate Device – NIPSCO recommends the definition change to remove "or collection of Cyber Assets." This limits the scope to only those assets that are used directly in the access control to assets subject to the CIP standards, rather than the broader "collection of Cyber Assets," which would include numerous cyber assets that an entity may deploy in a layered network architecture with numerous authentication points and isolation technology. i. Interactive Remote Access - NIPSCO recommends removing the 2nd sentence since the requirements specify the scope of applicability. The second sentence of the definition contains an applicability statement that is defining what remote access is not, and NIPSCO does not believe this adds any value to the definition and potentially introduces conflicts with specific architectures. j. Protected Cyber Assets – The proposed definition is unclear. NIPSCO therefore offers the following suggested language: "One or more Cyber Assets connected using a routable protocol within an Electronic Security Perimeter that is not part of the highest impact BES Cyber System within the same Electronic Security Perimeter." NIPSCO supports the Implementation Plan; however, recommends the removal of the Applicability Reference Tables as they do not appear to belong within an implementation plan document. NIPSCO does not support CIP-002-5 as proposed. The proposed language should be modified to specify that the applicable functional obligations referenced within R1.1 through R1.4, R2.11 and R2.12 apply to only those real time tasks identified in the Functional Model. NIPSCO also suggests that R1.3 be removed and that the Low categorization be eliminated. NIPSCO remains challenged with the approach of identifying the required Low assets within R1.3. The SDT has provided language to clarify that a discrete list is not required; however, NIPSCO seeks clarification on how an entity would demonstrate strict compliance with a requirement that directs an entity within the requirement to not create evidence. NIPSCO does not support CIP-003-5 as proposed. In R2, it is unreasonable to require an entity to

identify, assess, and correct the deficiencies of assets that it is not required to uniquely identify or inventory. NIPSCO seeks clarification on how an entity would demonstrate strict compliance with a requirement that directs the entity within the requirement to not create evidence. NIPSCO recommends removing this requirement. NIPSCO supports CIP-004-5 as proposed; however, NIPSCO recommends that the revocation periods for R5.3 and R5.4 be aligned to both be 30 days. Also, NIPSCO suggests that R5.3 should also apply to reassignments and transfers in addition to terminations and removal of access to BES Cyber Information. NIPSCO does not support CIP-005-5 as proposed. R1.3 should use the term "controls" instead of "permissions" to align with the measure language. Also, NIPSCO recommends changing R2.2 to "Interactive Remote Access sessions must utilize encryption to an Intermediate Device." This would allow for termination of the encrypted communication at the VPN concentrator without the requirement to have encryption to every intermediary device along the path from the remote user to the BES Cyber Asset. Finally, NIPSCO recommends changing R2.3 to "Interactive Remote Access sessions must utilize multifactor authentication to an Intermediate Device." This would allow for multifactor authentication to the VPN without the requirement to have multifactor authentication at every intermediary device along the path from the remote user to the BES Cyber Asset. NIPSCO supports CIP-006-5 as proposed NIPSCO does not support CIP-007-5 as proposed. R2.2: NIPSCO suggests changing the 35-days requirement to "monthly." NIPSCO interprets the current requirement language as likely creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation presumably would need to be tracked individually to ensure that the task is continuously performed 35 days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. For example, if an entity evaluated security patches for applicability for a set of systems on the 18th of October and then with the holidays in November they performed the task again on Nov 26th, it presumably would be out of compliance. Conversely, if the requirement stated "monthly" the entity presumably would be in compliance. Additionally, the tracking date of R2.2 has implications on the requirement date for R2.3. R2.3: If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. R2.3: NIPSCO suggests changing the 35-days requirement in R2.2 to "monthly." NIPSCO interprets the current requirement language as likely creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation presumably would need to be tracked individually to ensure that the task is continuously performed 35-days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. R2.4: NIPSCO believes that the language in R2.4 should be aligned with the language in R2.3. Either both or neither should specify the approval requirement of the CIP Senior Manager or delegate. NIPSCO recommends ". . . timeframe specified in Part 2.3 is approved." R3.1: NIPSCO believes that the use of the term "deter" is ambiguous and suggests removing the term from the requirement. R3.2: NIPSCO believes that the language used in the requirement is ambiguous. NIPSCO suggests replacing the language in the requirement to "Configure the measures implemented in R3.1 such that it blocks or prevents access to files with potentially harmful code." This recommendation is based on the assumption that the recommendation for removal of the term "deter" is accepted in R3.1. R4.1: NIPSCO recommends changing R4.1.2 to remove "failed access." The requirement would be "Detects failed login attempts." R4.2: NIPSCO recommends changing the language of R4.2.2 to "Detected failed login attempts from Part 4.1." 4.4: NIPSCO believes that the requirement is too ambiguous. It is unclear what would constitute a summarization or a valid sample. NIPSCO believes that the requirement to review 'undetected' Cyber Security Incidents is essentially a requirement to perform manual reviews. By requiring a manual review, the entities are encouraged to record the absolute minimum event types as to minimize the burden of the manual review. Further, the requirement to perform manual reviews would incentivize entities to not invest in systems that can perform automated log analysis and event correlation. 5.6: NIPSCO recommends that ". . . at least once every 15 calendar months" be replaced with "at least once each calendar year." NIPSCO supports CIP-008-5 as proposed; however, NIPSCO recommends the following addition to the language of R1.2: ". . . Initial notification to the ES-ISAC, which may be only a preliminary notice, shall not exceed one hour from identification of the Reportable Cyber Security Incident." This change adds clarity that the one-hour time frame begins when an incident is identified as a reportable incident. NIPSCO supports CIP-009-5 as proposed NIPSCO does not support CIP-010-5 as proposed. NIPSCO suggests that the 35-days requirement in R2.1 be changed to "monthly." The requirement should state: "Monitor at least monthly for changes to the baseline configuration. . ." NIPSCO interprets the current requirement language as creating a rolling 35-day period for each individual BES Cyber Asset, and the triggering documentation would need to be tracked individually to ensure that the task is continuously performed 35-days from the last time it was performed. Typical entity management programs would ensure that a task or set of tasks is completed within a month; however, the day of the month could vary based on holidays, vacations, system availability, and a number of other resource / process issues. The needed flexibility to manage our environments with a month-to-month time frame would be lost by moving to a prescriptive 35 day rolling window. For example, if an entity performed a baseline review task for a set of systems on the 18th of October and then with the holidays in November it performed the task again on Nov 26th, the entity presumably would be out of compliance. Conversely, if the requirement stated "monthly" the

entity presumably would now be in compliance. If the SDT prefers to not use the phrase monthly, then NIPSCO recommends changing the requirement to 62 days. NIPSCO supports CIP-011-5 as proposed; however, NIPSCO notes a typo in R 2.2 in the "Measures" section at the first bullet, i.e., remove "a" prior to "an."

NIPSCO believes the SDT has made significant improvement in the language and approach of the current V5 Draft 3. NIPSCO believes it is essential that the SDT continues on this path until industry approval is received in accordance with the Standards Drafting Process. These comments support the voting position of 4 NIPSCO voters in Segments 1,3,5,and 6.

Group

MRO NSRF

Joseph dePoorter

The MRO NSRF wish to make the following comments: CIP-002-5 R1 – For consistency and clarity, either remove the list of assets (1-6) and refer to the attachment or change R1.1 through R1.3 and R2.1 and R2.2to align the NERC filing in which NERC committed to using numbered or bulleted lists and which was approved by the Commission on May 19, 2011. Please change accordingly. CIP-002-5 through CIP-011-1, Applicability sections 4.1.2.4 and 4.2.1.4: Please strike "and group of Elements" as it is redundant with Cranking Path. By definition, the Cranking Path is "a portion of electric system that can be isolated and then energized to deliver electric power from a generation source". Cranking Path will include the "group of Elements meeting the initial switching requirements". Thus, the inclusion of this language is unnecessary and will only contribute to ambiguity. Distribution Providers will be forced to question if the drafting team intended to include something above and beyond the Cranking Path. CIP-002-5 R1 and associated VSLs: The requirement uses the term "assets" and the VSL uses the term "BES assets". Both the requirement and VSL should consistently use that same term. CIP-002-5 R1 Part 4 and Attachment 1 Criterion 3.4: Part 4 and Criterion 3.4 need to be modified to use language consistent with the EOP-005-2, EOP-006-2, and the Applicability section 4 of the CIP-002-5 through CIP-011-1 standards. Please change "blackstart generators" to "Blackstart Resources". Also, please change "substations in the electrical path of transmission lines" to "Cranking Path". Blackstart Resources and Cranking Path have specific meanings and are consistent with other standards. Use of terms that are not defined when specifically defined terms exists creates ambiguity in the meaning of the standard. It will cause registered entities to question if something else is meant by these terms. Furthermore, "substations in the electrical path of transmission lines" would not be consistent with the Applicability section regarding Distribution Providers since they will not have transmission lines. CIP-002-5 R2.1: Please modify "Review (and update as needed) the identification" to "Review the identification and update it if there are changes identified". Otherwise, it implies that the registered entity is to conduct additional reviews and updates whenever there might be a change which could compel the registered entity to continuously review its identification from Requirement R1. CIP-002-5 Attachment 1: Please change "System" to "system" in Criterion 2.9. It is not used consistently with the NERC Glossary definition. CIP-002-5 Attachment 1: Please add a qualifier to Criterion 3.1 that clarifies it only applies to BA and GOP control centers. All RC and TOP control centers will have been included in Medium and High Impact through criteria 1.1, 1.3, and 2.12. CIP-002-5 Attachment 1: In criterion 2.10, please strike "or group of Elements". Use of Elements is not consistent with the NERC definition. Elements are not typically components of a control system. Use of Elements here implies they are part of the control system for automatic Load shedding. The CIP SMET disagrees with the removal of "annual" obligations from all the Standards. The "once every 15 month" language can lead to a perception of loosened rigor around these activities, as it will allow entities to omit the activity for a calendar year. This decreases reliability and deviates from other NERC Standards. We recommend use of the term "annual," allowing the entity to define that term within its program. The definition of this term by the entity is consistent with an internal controls approach in mitigating security risks and provides a documented interpretation for the entity self-assessments and monitoring processes. An additional recommendation is to include the entity's definition of its "annual" cycles within the policy documentation required by CIP-003 R1. CIP-003-5 R2 – Rather than refer back to CIP-002-5, include the appropriate verbiage referring to assets containing low impact BES Cyber Systems. Recommend "Each Responsible Entity for itsassets that contain a low impact BES Cyber System(a discrete list of low impact BES Cyber Systems is not required)shall implement…" This aligns with the phrasing in CIP-003 R1 and CIP-002 R1.3. CIP-003 R3 – The CIP Senior Manager relies on both the definition in the CIP Glossary and the "Responsible Entity" verbiage in every Standard in section 4. There isn't a clear connection between these two, based on the inconsistent verbiage. Recommend addressing the definition or the verbiage in this requirement to allow a CIP Senior Manager to be based on the specific organizational structure. According to other risk management frameworks, Registered Entities should have flexibility in assigning the scope and responsibilities for CIP Senior Manager(s). CIP-003-5 R3 – The measure can be interpreted to mean that the person designating the CIP Senior Manager may have to be organizationally above the designee. In a small company, it might be reasonable that the highest level official designates him/herself as the CIP Senior Manager. This flexibility should be allowed and it should be clear within the verbiage of the measure. CIP-003-5 R4 – This requirement should not include the "identify, assess, and correct" language, as it is a results-based requirement where deficiencies are unlikely and, if they do exist, create a lot of risk for the organization related to unauthorized signatures. Also, strike the last sentence related to a change in the delegator. If either the delegator or the delegate changes, the delegations should be reviewed/updated. CIP-004-5 R2 – It is a security risk to address some of the concepts listed in 2.1.1 through 2.1.9 with every single person with a need for physical or cyber access to a cyber system, regardless of his or her role. This requirement should be broken out into those general concepts necessary for every access

type/role and those, more specific, concepts (2.1.8 and 2.1.9) that should be reserved for those with a role and are allowed after granting access and renewed annually. In the absence of that granularity, the training program could be ineffective due to the generic information that would be included to meet the requirement. However, in the absence of that approach, this requirement should be left at the current level of specificity (or lack, thereof), allowing the entity the flexibility to provide a minimal amount of training before granting access without requiring additional training afterwards. CIP-004 R4.3 – Provide clarity related to which accounts are subject to an annual review. Does this list of accounts include all of those enumerated in the guidance for CIP-007 R5 (p.43)? If so, this should be clearer. If not, is it the intention of the drafting team to omit that list of accounts from the annual and quarterly review requirements? CIP-005-5 R2.1, R2.2, and R2.3 – Add "Where technically feasible" to the front of both requirements. CIP-005-5 R2.1– This verbiage does not account for situations where the intermediate device can be locally accessed [a local administrator, for example] inside the PSP. This local access, due to the other restrictions around Intermediate Devices, will have the same security stance as someone remotely using the ID to get into the ESP. So, the verbiage in this requirement should account for local access to the ID. Recommend, "Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset, unless the Intermediate Device is used locally to directly access the Cyber Asset." CIP-005-5 R2.2 - This phrasing does not achieve the intention, which is to have traffic inspected by the IDS in an unencrypted state. So, if that's the intention, the phrasing needs to reflect that result, not the method, because this method, depending on the configuration, may not achieve the goal while it achieves compliance with the specific words. As technology changes, the method prescribed will become outdated. Instead, prescribe the result – encryption is part of the protocol with provisions for IDS efficacy. CIP-010-5 R1.4 – The "guesswork" initiated by CIP-010-5 R1.4.1 does not add value. This is especially true if the only thing that must be tested by R1.4.2 is the list of controls identified with the guesswork. The entity is enticed to round down. Recommend striking 1.4.1 completely and change 1.4.2 to say "Following the change, verify that cyber security controls are not adversely affected." Keep 1.4.3. CIP-010-5 R1.5 – We do not feel that emergency change controls necessary for reliability should be a TFE if related to a CIP Exceptional Circumstance. Recommend adding that verbiage to the beginning of the requirement. Alternatively, if it is the intention of the drafting team to indicate that a TFE is necessary if an entity doesn't have a test environment for a High Impact BES Cyber System, the TFE language should be moved down into the 1.5.1 or 1.5.2 to eliminate references to a TFE for each change.

None

Individual

RoLynda Shumpert

South Carolina Electric and Gas

1) The SDT should clarify their expectation on how low-impact BES Cyber Systems are identified in CIP-002-5 R1.3: Based on the definition of a BES Cyber System and BES Cyber Asset, an entity could find latitude with CIP-002-5 R1.3 to create an assessment methodology to determine whether it has any Low Impact BES Cyber Systems. If the entity can prove that the loss/compromise/degradation of each BES Facility identified under Part 4.2. and 4.3 has no impact on the overall BES, then the entity could justify having no Low Impact BES Cyber Systems identified for those parts. Was it the SDT's intent to accommodate this approach? Or, was it the SDT's intent that all cyber assets affiliated with the Facilities listed in Attachment 1 #4.2 and 4.3 be treated as Low Impact BES Cyber Systems, regardless of the Facilities impact on the BES? 2) For CIP-010-1 R2.1, extend monitoring period to 180 days. Depending on the number of BES Cyber Systems the 35 day requirement may become very burdensome to the BES Cyber Systems owners. If the BES Cyber Systems has a robust configuration management program every 180 days would be sufficient to document any change to the baseline. 3) Please provide clarity on the expectations of CIP-010-1 R3 Parts 3.1 and 3.2 in regards to the "High Impact BES Cyber Systems". Why does the "High Impact BES Cyber Systems" have two different time frames for an CVA (once every 15 calendar months and once every 36 calendar months). Both requirement could be met with a single CVA on the production environment. Correct? Was the intent to create a margin of variation to fit the Registered Entities systems? Or just an typographical error? 4) CIP 004-5, Table 5, Part 5.3 change rationale expects that BES Cyber System Information may reside in a file management system, but CIP 011-5 seems to assume it only resides on a BES system or in a PSP. CIP 010 requires testing of all changes if technically feasible, but in some cases a test environment may not be appropriate even if feasible. The operational exercise requirement in CIP 009-5 should be clarified, especially if failover could risk service interruption. The mitigation of the threat of malicious code in CIP 007-5 is too vague and leaves too much to the auditor's interpretation. The CIP 006-5 requirement for two or more different physical access controls may not always be practical or necessary even when it is technically feasible. CIP 005-5 should consider data diodes, possibly exempting systems with only a data diode connection from "external connectivity" provisions. The words "when technically feasible" should be added to CIP 004-5, Table R5, Part 5.5 to reflect the possibility that a device might have a hard coded password that cannot be changed.

Individual

Tracy Richardson

Springfield Utility Board

In the Draft CIP-006-5 RSAW, "deficiencies" are mentioned in terms of creating "low risk" or "high risk" to the reliability of the bulk power system. However, the CIP-006-5 Standard, nor any other related documentation,

appears to mention or provide guidance on how to determine risk to the bulk power system. Risk determination is only discussed in the RSAW, which states that non-compliance is to be left up to "his/her (CEA's) professional judgment". An individual's professional judgment does not promote any kind of consistent application of risk assessment.

Individual

Ed Nagy

LCEC

: (CIP-002-5 Requirement Attachment 1 – Do Not Support – R1 or Attachment 1 - 2.12) The bright-line criterion is too inclusive as it includes Control Centers of low/no impact Radial Transmission Operators (TOP) unnecessarily. The SDT has taken a position that in order to comply with FERC Order 706, Paragraph 280 that all TOP Control Centers MUST be identified as Critical Assets. In reality, FERC Order 706 states that "It is difficult to envision a scenario in which a TOP Control Center would not be identified as a Critical Asset." The Commission did not say that all TOP Control Centers MUST be identified as Critical Assets! The Commission clearly states that "Responsible entities should also examine the impact that misuse of those control centers could have on the ELECTRICAL FACILITIES THEY CONTROL and what the COMBINED impact of those facilities could be on the reliability of the Bulk-Power System. Since the bright-line criterion is replacing the responsible entities methodology, it is critical that the bright-line criteria also consider the impact of the facilities CONTROLLED by a TOP Control Center and the COMBINED impact of those facilities. CIP-002-5 Attachment 1 - 2.12 includes all TOP Control Centers as Medium Impact to the BES without regard for the COMBINED impact of the facilities controlled by the Control Center. This results in the applicability of Cyber Security Controls to Control Centers that do not impact the Bulk Electric System (BES). In CIP-002-5 Attachment 1 Requirement 2.5 Transmission Facilities are identified as Medium Impact to the BES if their "Aggregate weighted value" exceeds 3000. The SDT explains that this value is derived from weighted values related to three connected 345kV lines and five connected 230kV lines at a transmission station or substation. Attachment 1 - 2-12 includes TOP Control Centers as Medium Impact to the BES when ALL OF THEIR BES Transmission Lines COMBINED, DO NOT meet the Medium Impact requirement in Attachment 1 - 2-5. Including these TOP Control Centers as Medium Impact to the BES is not necessary; conflicts with FERC Order 706 and the rational used within CIP-002-5 Attachment 1 – 2.5 To "Include BES Cyber Systems for facilities at the lower end of BES Transmission with qualifications for inclusion IF they are deemed HIGHLY LIKELY to have SIGNIFICANT IMPACT on the BES."

In general, the Cyber Security Controls that are required for Medium and High Impact BES Cyber Systems are nearly identical. This results in a mismatch between the level of controls required and the impact to the BES. The impact of this is even more significant since entities that do not impact the BES are being included as Medium Impact based on the bright-line criteria.

Group

BC Hydro

Patricia Robertson

CIP-002-5 R1: BC Hydro requests clarification on the Applicability of Distribution Providers ie does 4.2.1 mean any DPs owning assets in this section must comply with the CIP standards? Are these the only DP assets that need to be considered for CIP compliance? CIP-002-5 R1: In a few of the bullet points within this section the wording "…is subject to one or more requirements in a NERC or Regional Reliability Standard" standard is used. Can the wording be changed to be more explicit as to naming the standards that the Registered Entity may be subject to (i.e. 4.1.2.2 and 4.1.2.3) CIP-002-5 R2: BC Hydro requests clarification on the term "associated data centers". Are these the "data centers" that service/support a control center? CIP-004-5 R3: BC Hydro has concerns with the personnel risk assessment program requirements, ie when performing ID verifications outside of the US and Canada it can be difficult and time-consuming (6 to 8 weeks) to conduct International ID verifications, assuming the information is available (which is not always the case), and suggests the following language be added to 3.1 (ID verification): "If it is not possible to perform a full ID verification (i.e. international) then the Registered Entity will document the reason the full seven year criminal history records check could not be performed." CIP-004-5 R3: When referencing the previous version the standard states "Specified that identity confirmation is only required for each individual's initial assessment." BC Hydro is requesting clarification that this is correct as this is not the most secure method (i.e. people can always create an alias so the ongoing checks should also include an ID verification. CIP-004-5 R4: BC Hydro requests clarification for the word "verify" – i.e. how would the Registered Entity be expected to provide evidence of access control ie evidence of proper access control to a locked cabinet that contains sensitive information – would a policy suffice? CIP-004-5 R5: 5.1: BC Hydro requests clarification for the word "removal" – is this meant to mean deletion or would disabling the access suffice. CIP-004-5 R5: 5.4: This section appears to be redundant. BC Hydro requests clarification on what scenarios would fall into this category that are not covered within 5.1 to 5.3. CIP-004-5 R5: 5.5: "For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action"; such a requirement could negatively impact the reliability of the bulk electric system in cases where there is a high movement of staff between locations. In such cases the password may change so many times that it impacts people's ability to access BES cyber systems (they forget the password due to the high change rate). CIP-007-5 R1: 1.2: "Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or

removable media." Introduction of physical port protection is "assumed" to refer to logical ports only. Can having strong physical access controls to BES Cyber System be a compensating control here? Will having the BES cyber systems in locked cabinets suffice? The requirement is not clear if the protection has to be on the individual devices. The measures indicate signage as a potential control however this would not satisfy the requirement the way the requirement is written. CIP-007-5 R4: "Review a summarization or sampling of logged events as determined by the Responsible Entity at intervals no greater than 15 days to identify undetected Cyber Security Incidents." BC Hydro requests clarification on the word "review". Would an automated SIEM technology solution, which monitors events in real-time, not satisfy this requirement? CIP-010-5 R1: BC Hydro assumes the test environment has to be a close representation to production but not an exact mirror and would like this confirmed. CIP-010-5 R2: "Monitor at least once every 35 calendar days for changes to the baseline configuration (as described in Requirement R1, Part 1.1). Document and investigate detected unauthorized changes." This requirement will be onerous and require significant effort without adding any significant security benefit. Would an effective change control process not satisfy compliance when paired with other controls that can mitigate the risk of unauthorized changes such as monitoring of unauthorized access via a SIEM technical solution?

BC Hydro voted Negative due to the issues provided for Question 1 and supports the rest of the standards/requirements.

Individual

Patricia Lynch

NRG Energy Inc.

CIP-002 BES System Categorization - No comments CIP-003 1.Background –and all standards where language for internal controls state that" each entity shall implement, in a manner that identifies, assesses and corrects deficiencies"- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. CIP-004 1.CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. CIP-005 No comments CIP-006 1. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection." CIP-007 No comments CIP-008 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include "as applicable". CIP-009 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. CIP-010 No comments CIP-011 No comments DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center

Group

Florida Municipal Power Agency

Frank Gaffney

FMPA appreciates the hard and excellent work of the SDT to significantly improve the CIP standards and develop a prudent method to protect the Bulk Electric System from cyber attacks. Although we have several comments, only one comment is causing us to vote Negative for any of the standards. CIP-002-5, Attachment 1, Bullet 2.12: The SDT added thresholds for Control Centers for small GOPs and small BAs to define a boundary between "Medium" and "Low" Control Centers, but no equivalent threshold for small TOPs, which is inappropriate. Why would a small control center controlling 1499 MW of generation be "Low" whereas a small TOP's control center for two 138 kV substations with only four 138 kV Facilities be "Medium"? We suggest that a threshold be added for small TOPs to distinguish between Medium and Low. The threshold can be design similar in concept to bullet 2.5, but including >100 kV and <200 kV Facilities with a score of 350. In this way, all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low.

These are issues that FMPA believes ought to be fixed, but are not causing us to vote negatively. Zero-Defect solution doesn't get us all the way there: The helpful phrase: "shall implement, in a manner that identifies, assesses, and corrects deficiencies, one or more documented … policies" was added to many requirements to try and address the "zero-defect" problem. However, by choosing the active word "implement", the zero-defect problem is reintroduced. "Implement" means: "to fulfill, perform, carry out", which means that in order to prove that a policy was carried out, detailed evidence of the results of executing the policy is needed, reintroducing the zero-defect problem. FMPA recommends replacing the word "implement" with "institute" which means "to set into

operation" or "to bring into practice or use" for which the evidence would be less onerous (e.g., the policy itself and proof that it was instituted, such as procedures that support the policy) avoiding reintroduction of the zero-defect problem. CIP-002-5, R1: How is an auditor to verify identification of all BES Cyber Systems that are applicable to R1.1 and R1.2? FMPA waits with interest on what the RSAW will look like. CIP-003-5, R4: The SDT seems to intend to address the zero-defect issue; however, by not associating the documentation of delegation contained in the 3rd sentence to the process of the first sentence, the goal is not accomplished and a strict reading of the requirement still includes a zero-defect problem of needing to document delegation for every delegation and delegation change within 30 days because there is more than one requirement embedded in R4. CIP-006-5, R1: The standard does not answer the question "how big does an opening in the Physical Security Perimeter have to be before is it deemed an access point"? It seems the SDT wants to use the 96 square inches used by some defense agencies, if so, we recommend explicitly stating that in the standard. CIP-006-5, R1.9 and R2.3, CIP-007-5, R4.3, CIP-008-5, R2.3: These are data retention requirements and should not be requirements of the Standard, especially considering the Paragraph 81 effort which is seeking to retire requirements just like this. CIP-006-5, R2.1: The measure does not match the requirement. The requirement is for "continuous escorted access", the measure describes evidence at discrete points in time, not continuous. How is an entity to prove that a visitor was continuously escorted? Does this essentially mean video surveillance? Or written attestations of the person providing the escort?

Group

Duke Energy

Greg Rowland

Duke Energy supports the proposed 10 standards, the implementation plan, and the definitions.

CIP-002 Guidelines and Technical Basis; Requirement R1; Attachment 1; Overall Application; First Bullet: The last few sentences of this bullet make several references to the term "BES Asset". Duke Energy believes this is an artifact from previous drafts and should be replaced with a more current term. CIP-002 Guidelines and Technical Basis; Requirement R1; Attachment 1; Medium Impact Rating; Generation; Criterion 2.13: Duke Energy recommends the removal of the last sentence referencing 300 MW. Duke Energy believes this is an artifact from previous drafts. CIP-003; Requirement R2: Duke Energy recommends that the word "assets" be replaced with "Low Impact BES Cyber Systems" such that the policy will not conflict with other policies required at a site that also houses Medium or High Impact BES Cyber Systems. CIP-004; Requirement R1.1: Duke Energy recommends that "cyber security practices and physical security practices" be changed to "cyber security practices and/or physical security practices" to allow entities flexibility in crafting meaningful and unique awareness communications. CIP-004; Requirement 3.1: Duke Energy recommends that the Interpretation concerning the need to only perform an initial identity verification be incorporated into the requirement as opposed to the guidance document. Duke Energy recommends rewording the requirement to, "Process to confirm identity. This process needs only to be performed prior to initially granting access and does not require reconfirmation during the tenure of employment.". CIP-006; Requirement 1.7; Duke Energy would like to request clarification on why the wording in Requirement R1.7 differs from that in Requirement R1.5. Specifically, why does R1.5 specify alerting "within 15 minutes of detection" whereas R1.7 specifies alerting "within 15 minutes of the unauthorized physical access"? CIP-006; Guidelines and Technical Basis; Requirement R1; Methods to monitor physical access; First Bullet: Duke Energy recommends modification of the last sentence to read "These alarms must provide for notification within 15 minutes to personnel responsible for response" to align with the requirement. Immediate appears in the guidelines but not in the requirement itself. CIP-006; Guidelines and Technical Basis; Last Paragraph: Duke Energy recommends striking this statement concerning outage records. Outage records are not required to be maintained within the current set of requirements. CIP-007; Guidelines and Technical Basis; Requirement R4; R4.1: Duke Energy recommends clarification around the last two sentences. Currently, it refers to an entity which neglects to enable logging would be in violation. Per the Background section, a sole instance of failure is not grounds for a violation so long as it is adequately identified, assessed, and corrected. The statements in the Guidelines seem to be relics of a previous draft which conflict with the new approach. CIP-010; Requirement R3.3; Duke Energy recommends rewording the requirement to, "Prior to adding a new applicable Cyber Asset…" to clarify that this requirement only applies to Cyber Assets meeting the criteria in the Applicable Systems section and would not include a Cyber Asset that is temporarily connected for less than 30 days for the purposes of troubleshooting, eg. Definitions Document; BES Cyber System: Duke Energy requests clarification on the definition of BES Cyber System. Can a non-BES Cyber Asset be placed into the logical grouping of a BES Cyber System so long as the BES Cyber System contains at least one BES Cyber Asset? Currently, the definition would not support such an inclusion, but Duke Energy believes the intent is there such as to afford protections to such non-BES Cyber Assets as part of a larger logical grouping where appropriate. Definitions Document; CIP Exception Circumstance: Duke Energy requests clarification on the term "mutual assistance agreement". Definitions Document; Physical Access Control Systems: Duke Energy requests justification for the inclusion of the word "alert" as it did not appear in earlier drafts. Duke Energy recommends that because this was added late, it should simply be removed. Implementation Plan; Scenario of Unplanned Changes After the Effective Date; Duke Energy requests clarification of the term "Effective Date" and its usage in the title of this table. Is this the Effective Date of Version 5 or the Effective Date of a change or something else?

Individual

Anthony Jablonski

ReliabilityFirst

Even though ReliabilityFirst votes in the Affirmative for the Version 5 of the CIP Standards since we believe it is a much improved version and provides a "net gain" to bulk power system (BPS) reliability; the standards still focuses on defining the applicability of cyber security assets and controls using BPS reliability criteria. ReliabilityFirst offers the following comments for consideration: CIP-002-5, Section 5 Background, states "This standard provides "bright-line" criteria for applicable Responsible Entities to categorize their BES Cyber Systems based on the impact of their associated Facilities..." This may still be a fatal flaw in the methodology. Examples are: • BPS assets (facilities, elements, etc.) not categorized as high or medium impact default to low impact and do not require discrete identification. Under the low impact categorization, the associated BES Cyber Assets and BES Cyber Systems at these BPS Assets will be protected only in the areas of cyber security awareness, physical access control, and electronic access control and the entity will have obligations regarding incident response. These are not the full complement of CIP Standard and Requirement security controls and provide a very basic or rudimentary set of security controls that may not provide an adequate level of protection due to the "electronic interconnectedness" of these systems with BES Cyber Assets and BES Cyber Systems categorized as high or medium impact. Weak cyber security controls applied to the low impact BES Cyber Systems can have adverse security and reliability related impact on those BES Cyber Systems categorized as high or medium impact. Secondarily, as these low impact assets do not require discrete identification, the compliance monitoring of the associated BES Cyber System security controls will likely be only the verification of program level policies and not actual testing of implemented security controls. This provides very little assurance that these assets are properly protected. • CIP-002-5, Section 5 Background: Real-time Operations, states "To provide a better defined time horizon than "Real-time," BES Cyber Assets are those Cyber Assets that, if rendered unavailable, degraded, or misused, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise." A compromise of any BES Cyber Asset can have an immediate (far less than 15 minutes) impact on the affected BPS Asset and any interconnected BES Cyber Assets and Systems with the potential for far reaching impact. Again, in this instance we are defining cyber security asset applicability using reliability criteria. A 15 minute window for operations staff to assess and take automated or manual action makes sense from a reliability perspective. To say a Cyber Asset is only declared a BES Cyber Asset if it would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise does not consider how all instances of cyber compromise can be attempted and then realized. Again, due to BES Cyber System interconnectedness, a BES Cyber System may be compromised with no immediate impact, only that it has been compromised for later malware activation or for deeper reconnaissance into the control system network. A 15 minute window means nothing regarding identification of BES Cyber Systems and Assets that can have an adverse effect on BPS reliability. Ultimately, with BPS Asset reliability criteria defining the applicability of cyber security assets and therefore those that will be protected with appropriate security controls, the risk and impact of interconnected SCADA and ICS may never be fully assessed or taken into consideration. The focus for the CIP Standards should be placed on the identification of all BES Cyber Systems and associated BES Cyber Assets, their interconnectedness; and the reliability operating services they support such as Control, Monitoring, Situational Awareness, Inter-Entity Real-Time Coordination and Communication, etc. This model will provide for more "full featured" cyber security that supports reliability without any gaps. The NRC Cyber Security model detailed in 10 CFR 73.54 including Regulatory Guide 5.71 may provide a relative comparison by which to reassess and rewrite the NERC CIP Standards.

Individual

Jianmei Chai

Consumers Energy Company

CIP-002 rev 5 and Attachment 1 Section 3.4 of the Attachment 1 is inconsistent with the requirement in CIP-002-5 Section 4.1.2.4. The two sections speak of the same Black-Start/Restoration Plan cranking path(s), yet describe each differently, potentially leading to different outcomes. Additionally, it would seem that with the current wording, all cranking paths (as 4.1.2.4 says "Each") identified in the Restoration Plan, which could be used as part of the initial restoration efforts, would need to comply. The requirement, in both Section 4.1.2.4 and Attachment 1, Section 3.4 should read specifically that only the initial "Primary Cranking Path" be included for compliance. Also, Paragraph 3.4 uses the phrase "… in the electrical path of 'transmission' lines used …", in describing the restoration path. There needs to be clarification on whether this solely applies to Transmission (capital T) or any and all lines in the path. If the latter, Consumers Energy recommends striking the word "transmission" entirely. Again, the rewrite needs to be consistent with section 4.1.2.4. Additionally, the Functional Entities in section 4.2.1.3 and the Impact Rating Criteria in Attachment 1, section 3.6, for Distribution Providers to include facilities containing "A Protection System that applies to Transmission …" is a new (initially introduced in draft 2) unsubstantiated requirement for Low Impact assets. The requirement should be deleted, or if such assets are to be included, the "applies to Transmission" phrase needs to be better defined, and only those assets/systems that can have a significant impact, such as impacting one or more Interconnection IROLs, should be included. Consumers Energy suggests wording pertaining to the IROLs similar to that found in section 2.9. Section 4.2.2 indicates that all BES facilities be included. Consumers Energy recommends that the criteria specified in section 4.2.1 for Distribution Providers also apply to Generation Resources. By not including this specific criteria, the scope of assets included in CIP Version 5 significantly increases from CIP Version 4. This seems excessive, as Generation

Resources often fall off-line without any adverse impact on the BES. Therefore, it makes sense to only include Generation Resources that would be most likely to have an adverse impact on the BES, which would be those specified in 4.2.1. Attachment 1 (of CIP-002) Attachment 1, Section 2.1, states "Commissioned generation, by the each group of generating units at a single plant location…." The use of the word "by" in this sentence does not make sense and should be reworded. Attachment 1, Section 3.3, lists "Transmission Substations and Stations" and "Generation Resources" in the list of Low Impact Cyber Systems at Facilities requiring compliance. Without the ability to perform a risk-based assessment any longer (as in CIP versions 1-4) all such Facilities will have cyber assets regulated (and regulated the same, regardless of importance) unless an entity can show that the cyber systems at these facilities will not meet the rather vague (see additional comment below) definition of BES Cyber Asset, and thus not qualify at all as a BES Cyber Asset. The definition currently does not provide adequate help in identifying assets and therefore the result of section 3.3 will be, as a minimum, to include all Transmission Substations/Stations and BES Generation Resources in the low impact category, thus requiring compliance. As noted below, Consumers Energy believes that modification to the BES Cyber Asset definition will correct this deficiency. Lastly, Consumers Energy recommends a minor modification to section 3.6 for clarity, such that it read "… Protection and UFLS and UVLS systems, specified in the Applicability Section 4.2.1, above." CIP-003 rev 5 Requirement R2 requires entities to have some protection for any BES Cyber Asset/System, regardless of actual impact that the cyber asset may have on facilities determined to be "Low Impact". In spite of numerous comments to the contrary provided to the SDT in previous drafts, this aspect of rev 5 remains. This would infer that all such low impact cyber/programmable devices are of the same value or importance of function to BES reliability, but this is far from true. In the proposed standard, a configurable electronic panel meter (providing local, seldom-used indication) in a substation, would potentially rise to the same level of compliance (albeit "Low") as an RTU or protective relay in that same substation. In this regard, Consumers Energy recommend that the SDT consider developing bright-line criteria that could be used for defining BES Cyber Assets at different levels based on the asset's impact of MW levels, system disturbance potential, or other substantial BES events. Back in CIP-002, rev 5 - Attachment 1, Section 2, (and especially item 2.5) the SDT seems comfortable eliminating applicability for facilities of lower voltages or MW value. It would seem nonsensical to then include cyber assets at other facilities, if the impact on reliability due to a compromised cyber asset was equally as small or even minute. The Definitions document The Definition of a BES Cyber Asset continues to be vague, in spite of past comments to the SDT. In rev 5 draft 3, it states: BES Cyber Asset A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems. (A Cyber Asset is not a BES Cyber Asset if, for 30 consecutive calendar days or less, it is directly connected to a network within an ESP, a Cyber Asset within an ESP, or to a BES Cyber Asset, and it is used for data transfer, vulnerability assessment, maintenance, or troubleshooting purposes. The use of "adversely impact" and "reliable operation" in this definition is particularly vague. Instead, it has been previously recommended that the SDT use a more definitive definition regarding the impact/effect of a cyber event, or one providing 'bright-line' criteria, but the definition has remained essentially the same again in draft 3. At this time, Consumers Energy proposes the inclusion of the NERC Glossary term, "Adverse Reliability Impact" in place of the two phrases. The Adverse Reliability Impact definition is fairly specific, concise and states: Adverse Reliability Impact Current FERC-approved definition: The impact of an event that results in frequency-related instability; unplanned tripping of load or generation; or uncontrolled separation or cascading outages that affects a widespread area of the Interconnection. Recently NERC BOT-approved definition: The impact of an event that results in Bulk Electric System instability or Cascading. Without the use of the Adverse Reliability Impact definition, the SDT unilaterally and significantly extends the potential scope of cyber assets being regulated, in both our HVD and LVD DCO, and Generation facilities. The Cyber Asset and BES Cyber System definitions do not consider if or how "programmable electronic devices" can be accessed or are connected. Consumers Energy recommends adding additional clarification similar to that in CIP Version 3, CIP-002 R3.1, "The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter."

In revision 5, draft 3, the SDT has revised the use of the Reliability Operating Service to no longer be a NERC defined term, but maintained the concept of the same. The continued use of the reliability operating service in the Application Guidelines, as a guide or aid in determining BES Cyber Systems should be discontinued. The concept is highly subjective and opens the door to numerous areas of increased scope in the standards applicability. As noted earlier by Consumers Energy, the SDT should instead refer to and use the very well-defined term, "Adverse Reliability Impact" for determining which cyber assets/systems may impact the BES.

Individual

Scott Berry

Indiana Municipal Power Agency

Control Center – IMPA does not support the definition of Control Center. The definition uses the words "monitor and control" and when it comes to defining what is included in those words the SDT has told the industry to reference the FAQ Document for Cyber Security Standards CIP-002 –CIP-009 (May 9, 2005). In this document, the answer to question 12 (page 5 of 24) states that "monitoring and operating control function includes controls performed automatically, remotely, manually, or by voice instruction." IMPA does not agree with including

"manually or by voice instruction" in this usage and then apply it to the definition of Control Center. The consequences of using these words will make many small entities have new Control Centers, and they will have BES Cyber Assets due to having a simple wired telephone or a wired fax machine that can have numbers programmed into it (the definition of a Cyber Asset covers programmable electronic devices). This could lead to many small entities owning TOP or GOP Control Centers because generally most of them do perform reliability tasks for transmission or generation at two or more locations. In addition, the loss of a telephone could lead to not starting or stopping a 20 mva generating unit (connected to the BES at 100kV or above) which an auditor could judge as having an adverse impact because it is a registered BES Facility. This scenario is unlikely due to entities having backup communications (another land line or cell phone communications) but when it comes to the evaluation of a telephone it states under BES Cyber Asset that "Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact." IMPA does not support the use of manual or voice instructions (especially voice instructions) when it comes to the terms "monitor and control" in the definition of Control Center and recommends updating these terms from a document written in 2005 in a new document to reflect the removal of them.
no comment
Group
Tampa Electric Company
Ron Donahey
Tampa Electric (TEC) wanted to thank the SDT for the hard work and energy that the SDT have put in during the development of version 5, despite the many challenges along the way. We support the intent and overall direction that the standards take. For CIP-002 R 1.3, TEC believes the intent is to provide protection at BES Facilities that do not meet the Attachment 1 Criteria 1.1 through 2.13. However, we believe that the CIP-002-5 R1.3 wording is technically flawed and conflicts with the definitions of BES Cyber Assets/Systems. By definition, to qualify as a BES Cyber Asset/System the asset must have a 15 minute impact on reliability of the BES. However a low impact facility cannot have such an impact to the BES per the attachment 1 criteria. Based upon this reasoning, we believe it is not possible to have a facility that meets the criteria of CIP003 R1.3.
Tampa Electric (TEC) wanted to thank the SDT for the hard work and energy that the SDT have put in during the development of version 5, despite the many challenges along the way. We support the intent and overall direction that the standards take. For CIP-002 R 1.3, TEC believes the intent is to provide protection at BES Facilities that do not meet the Attachment 1 Criteria 1.1 through 2.13. However, we believe that the CIP-002-5 R1.3 wording is technically flawed and conflicts with the definitions of BES Cyber Assets/Systems. By definition, to qualify as a BES Cyber Asset/System the asset must have a 15 minute impact on reliability of the BES. However a low impact facility cannot have such an impact to the BES per the attachment 1 criteria. Based upon this reasoning, we believe it is not possible to have a facility that meets the criteria of CIP003 R1.3.
Individual
Michael R. Lombardi
Northeast Utilities
Northeast Utilities (NU) supports all 10 of the proposed (draft 3) CIP V5 standards, the implementation plan, and the set of definitions.
In addition to our support, Northeast Utilities offers the following comments for your consideration: We assume Draft 3 is relatively stable, yet for CIP-004-5, Part 5.2, the revocation of an individual's access "by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access" is administratively burdensome without a corresponding benefit to reliability. We suggest the "by the end of the next calendar day" be replaced with "within 30 days." Since there is a low risk to physical or cyber security. CIP-006-5, Part 1.7, 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." Please clarify that statement, especially the personnel to be notified. Is notification automated, manual, or is it our choice? Additionally, please clarify if cabinets inside a PSP require individual alarming. NU recognizes that compliance with CIP V5 Standards will be a multimillion dollar effort. NU encourages NERC to institute compliance changes that clearly improve physical and cyber security to justify the capital and O&M costs the industry will incur.
Individual
d mason
HHWP
For us, the addition of the following language to the implementation plan for unplanned changes resulting in a higher categorization only muddles the timeline for compliance: "...with additional time to comply for requirements in the same manner as those timelines specified in the section 'Initial Performance of Certain Periodic Requirements' above."
Group
Dairyland Power Cooperative

Tommy Drea
Group
PPL Corporation NERC Registered Affiliates
Brenda Lyn Truhe
The PPL Companies thank the Standards Drafting Team for their work on CIP Version 5. Please consider the following comment for CIP-004-5 Table R5 – Access Revocation. In Part 5.4 - Applicable Systems, should PACS also be listed here? We ask as some cyber assets in a PACS can also have individual user accounts. We have the same comment for Part 5.5. Additionally, CIP-007-5 Part 5.5 Requirements, the first paragraph uses the term "interactive user access". This is not a defined term; however, it is similar to the CIP V5 Definitions defined term Interactive Remote Access. Should the term "interactive user access" be defined or clarified in the Guidelines and Technical Basis? CIP-003 states "An inventory, list or discrete identification of low impact BES cyber systems is not required." CIP-005 Guidelines and Technical Basis states an ESP is required around networks even if standalone regardless of impact classification. Please confirm the requirements in CIP-005 do not imply a list of Low Impact assets is needed.
Individual
Benjamin Smith
Tampa Electric
Project 2008-06 Successive Ballot CIP-002-5 September 2012_in, please refer to comments of Ron Donahey of Tampa Electric
Individual
Don Schmit
Nebraska Public Power District
Individual
Kevin Koloini
American Municipal Power
Group
Bonneville Power Administration
Chris Higgins
BPA believes CIP-002-5 is unclear. Attachment 1 doesn't specify where within-hour generation and interchange scheduling systems related to Balancing, Managing Constraints, and Inter-Entity Coordination fall within the high-medium-low impact framework. Impacts on IROL identification and BA, TOP, and GOP planning systems feeding real-time operations are also unclear. BPA reiterates previous comments and will seek clarity post-balloting. CIP-003-5 – R2 uses the term 'asset', this term is not defined by NERC and may be misinterpreted without definition. BPA believes CIP-003-5 R2 is referencing R1, part 1.3 of CIP-002-5, not R2, part 1.3 which doesn't exist. Suggest rewording R2 to remove the term "asset" and correct the reference to CIP-002-5. CIP-005-5 – BPA understands the valid security reasons for the requirement for access control on outbound connections, and has concerns with impact this will have on our ability to operate as required. BPA requests more clarity regarding the types of devices that would qualify as intermediate devices, beyond the requirements that they must support encryption for any interactive sessions and multifactor-authentication for access to any interactive sessions. Definitions – Please reconsider previous comments for Cyber Security Incident, BES Cyber Asset, Critical Assets and define "programmable" in "Cyber Asset".
Individual
Doug Hohlbaugh
FirstEnergy
FirstEnergy (FE) is conditionally approving and voting affirmative to the complete set of the CIP Version 5 standards. Our voting position is based on clarifying text that we believe must be added to the CIP-005-5 Guidelines and Technical Basis section for Requirement R1 (specifically parts 1.3 and part 1.5) to remove the operational barriers that may prevent Entities from implementing encryption among sites on a BES Cyber System network using either encrypted tunnels or tunnel-less encryption technologies. FE believes that NERC shares the opinion that the plain language of the standards should encourage the implementation of encryption technologies on critical networks. Consequently, FE proposes the following text (see ITEM 1) for the CIP-005-5 Guidelines and Technical Basis section for Requirement R1. At the discretion of the SDT, language may need to be added to CIP-005-5 R1.3 and R1.5 if that is required to ensure clarity in the formal Standards to support the audit process. ITEM 1: "Some Entities employ encryption as a strong measure for securing communications among discrete physical sites (e.g. data centers and control centers). Encryption (either via encrypted tunnels or group encrypted transport) effectively satisfies the establishment of 'discrete Electronic Security Perimeters' as referenced in Section 4.2.3.2 of each Applicability section. Provided the termination points of the encryption are protected within

Physical Security Perimeters, the requirements for CIP-005-5 R1.3 (inbound & outbound access permissions and deny-by-default) and CIP-005-5 R1.5 (inbound & outbound malicious traffic inspection) may be achieved at central firewall(s) protecting the BES Cyber System network to which the ESPs are connected. For traffic communicating within the encrypted network, the CIP-005-5 R1.3 and CIP-005-5 R1.5 requirements do not need to be duplicated at the encryption endpoints. This enables effective implementation of encryption, which might not otherwise be operationally feasible if traffic inspection were required inside of the protected network due to the latency and convergence delays that are introduced." ITEM 2: Additionally, FE understands that serially connected cyber assets would not be considered to be within an Electronic Security Perimeter (ESP) nor are they in scope for requirements applicable to BES Cyber Systems with External Routable Connectivity. Regarding the ESP, we come to this conclusion from reading of the standard drafting team's response to comments for Question B12 related to CIP-005-5 Requirement R1 which states "CIP-005-5, however, is focused on those two higher risk forms of connectivity and do not have mandatory requirements on serial, non dial-up forms of communication." Regarding the "… with External Routable Connectivity" applicability FE understands this to also excludes serially connected devices based on information listed in the Background section (Section 5) under the heading "Applicable Systems Columns in Tables". As an example, "Medium Impact BES Cyber Systems with External Routable Connectivity – Only applies to medium impact BES Cyber Systems with External Routable Connectivity. This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." We conclude that serial are not in scope when this applicability is used based on the second sentence that states "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." While it's understood that serially connected devices are in scope for other areas of the CIP V5 standards, FE requests that the standard drafting team confirm or clarify FE's view related to the ESP and the "w/ ERC" applicable items. ITEM 3: FE notes that within each Background section (Section 5) under the heading "Applicable Systems Columns in Tables" that the defined applicability statement for "Medium Impact BES Cyber Systems with External Routable Connectivity" is consistently stated throughout the CIP V5 standards with the exception of CIP-004-5. In CIP-004-5 the statement is missing the second sentence that appears in the other standards where Medium Impact BES Cyber Systems with External Routable Connectivity is also referenced in the Background sections. ITEM 4: These comments are supported by the following FE Registered Ballot Body personnel which include Segment 1 – William J. Smith; Segment 3 – Stephan Kern; Segment 4 – Douglas Hohlbaugh; Segment 5 – Ken Dresner and Segment 6 - Kevin Querry.
FE appreciates the hard work of the drafting team and the effort given moving from Draft 2 to Draft 3 is evident. Most notably, changes made to address various "zero defects" issues and allowing entities to implement strong internal compliance programs that include corrective action programs is a significant step forward. We offer the following additional comments to further improve the CIP V5 standards. ITEM 1: CIP-002-5 Background Section – The sentence that states "In transition from Version 4 to Version 5, a BES Cyber System can be viewed simply as a grouping of Critical Cyber Assets" should be struck or reworded. A BES Cyber System can be vastly different due to the removal of connectivity exclusions (non-routable) that exist in CIP V4. ITEM 2: CIP-007-5 R3, part 3.1 – Consider adding "Per device capability," to the beginning of the requirement. Otherwise, if a deter posture is selected, potentially in conflict with other requirements (e.g. 4.1). ITEM 3: CIP-010-1, R1, part 1.1.4 – Consider limiting the applicability for Medium to only those with External Routable Connectivity for consistency with CIP-007-5 R1, Part 1.1 ITEM 4: Background Section (ALL) – The statement that bulleted lists are "or" and numbered are "and" should be deleted. The list should be clear by direct reading within the standard. ITEM5: CIP-004-5 R5, Part 5.5 – Consider indicating within 35 days for consistency with other monthly requirements (e.g. CIP-007-5 R2, part 2.3).
Individual
Tony Kroskey
Brazos Electric Power Cooperative
Individual
Daniel Duff
Liberty Electric Power LLC
CIP-004: Please refer to detailed comments from the last round of balloting. Smaller entities rely on remote vendor support,and the lack of a method for allowing such support will result in a less reliable bulk electric system. CIP-007: Including specific password requirements in a standard that will take years to modify insures that new and safer technologies cannot be implemented by the industry, and again negatively impacts the reliability of the BES. Definitions: Control Center should be redefined. See the comments of Indiana Municipal Power Agency.
Individual
Darryl Curtis
Oncor Electric Delivery Company
N/A
Oncor supports the shift in compliance to the internal controls approach and we look forward to NERC providing a programmatic/principles framework in a collaborative approach with the industry. In the absence of this framework, it is unknown how the concept of "identify, assess and correct" will evolve. As the framework is

developed including the "identify, assess and correct" concept, Oncor requests that continuous focus be placed on implementing principles including this concept and not requiring or specifying internal controls which would place additional compliance burden on entities. The internal controls principles/framework should enable entities to establish internal controls model utilizing deficiency correction approach but should not mandate the approach. Internal Controls Program needs to be defined by an Entity, it is not a "One Size Fits All". The standards/RSAWs should reflect this understanding.
Individual
Robert W. Roddy
Dairyland Power Cooperative
Individual
Travis Metcalfe
Tacoma Power
Definitions: Control Center The relocation of the term "including their associated data center" reduces the clarity of Control Center and should be clarified to address two issues: 1. The word "associated" provides no guidance as to whether this is association by ownership, functionality or physical location. If the intent suggested on page 20 of the consideration of comments is to only cover data centers at the same physical site as the control center, the term should read "including their onsite associated data center." If the intent suggested on page 30 of the consideration of comments is only to cover data centers owned by the same owner as the control center, the term should read "including their associated data center(s) owned by the registered entity." Unfortunately both of these approaches could allow registered entities to avoid many CIP compliance requirements simply by outsourcing or physically relocating data centers. 2. Although the SDT suggests that many definitions of data center exist, they are not clear enough to separate out the typical equipment in substation control rooms & communication hubs versus the more complex equipment in a SCADA data center. For example, a transmission substation control will likely include every item listed in the wikipedia definition: "A data center or computer center (also datacenter) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices." BES Cyber System Information Tacoma Power supports removing the ambiguous phrase "pose a security threat." Page 23 of the consideration of comments states "the SDT does feel that it is prudent to remove this phrase," however it still appears in the latest revision. CIP-002 Section 4.2.2 -Applicability The capitalized term "Facilities" in "All BES Facilities" would to include only assets with electrical terminals and does not include items such as Control Centers, data centers, SPS/RAS or protection systems. As used elsewhere within the CIP standards, lower case "facilities" would apply more broadly. Appendix 1- section 3.2 "Low Impact Rating" Replace "Transmission substations and stations" with "Transmission substations and transmission switchyards" or with "Transmission stations." It is currently unclear why both stations and substations are listed. It is also ambiguous whether transmission applies to both terms, or just the first. CIP-006-5 R1.7 Comment and Recommendation Comment – The PACS associated with High or Medium Impact BES Cyber Systems is not an applicable system to the CIP-008-5 Incident Reporting and Response Planning requirement, therefore will not have responsible personnel identified in the BES Cyber Security Incident Response Plan. Recommendation – Change requirement language to read as follows: 1. "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to responsible personnel identified in the CIP-006-5 R1 Physical Security Plan within 15 minutes of the unauthorized physical access." Or more simply: 2. "Issue an alarm or alert in response to detected unauthorized physical access to a Physical Access Control System to responsible personnel within 15 minutes of the unauthorized physical access."
Group
SPP and Members
Lesley Bingham
SPP does not find sufficient deficiencies in any of the standards, the implementation plan or the set of definitions to vote against them.
CIP-002-5 Requirement 1 How is an entity to comply with both the "consider each of the following assets" section of Requirement 1 and adhere to the criteria for review in Attachment 1? CIP-002-5 Attachment 1 provides much detail for assisting many of the Responsible Entities classify assets into a High, Medium or Low Impact to the Bulk Electric System. However, there is no such guidance for the Transmission Operator (TOP). In the current draft of Attachment 1, TOPs of all sizes are considered as either High of Medium Impact. Smaller TOPs do not have the same impact on the BES, but will incur similar costs to implement their CIP compliance programs. Was a cost-benefit analysis done on the impact of CIP compliance for NERC and the TOPs, focusing on the needs of smaller operators? CIP-005-5 Requirement 1.2 The definition of External Routable Connectivity does not anticipate a situation where serial protocol may be used over IP connectivity. This may happen to provide flexibility of routing design, but may not strictly comply with the External Routable Connectivity definition. As an example, communication between two devices may take advantage of the Ethernet ports on the devices, but run serial protocol between the devices. The devices aren't using ip and the connections must be programmed internally to

use serial protocol. By explicitly stating, "routable protocol connection" in the definition and focusing an auditor's attention on the connection, the auditor may see the Ethernet port being used and determine noncompliance. Recommend deleting the word "connection" at the end of the definition of External Routable Connectivity. Requirement 1.5 is still geared towards implementing an IDS/IPS. An IDS would not provide the additional protection for an Electronic Security Perimeter (ESP) if a firewall failed, which seems to be called for in the FERC Order. Also, an IDS or IPS would provide no protection against an insider threat. 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, traffic patterns or signatures. Requirement 2.1 We would request clarification that the Interactive Remote Access must not be initiated from a device which allows direct access. Suggest the language "Utilize an Intermediate Device such that the Cyber Asset initiating Interactive Remote Access does not initially directly access an applicable Cyber Asset." Requirement 2.2 We would request clarification on whether the "Intermediate Device" is expected to provide the encryption or if two devices are envisioned for compliance. Requirement 2.3 We would request clarification on whether the multi-factor authentication is required for the Intermediate Device, for access to the Electronic Access Point or to the individual Applicable Systems. Suggest the language "Require multi-factor authentication for initiating all Interactive Remote Access Sessions." CIP-006-5 Requirement 1.2 The "5. Background" section of CIP-006-5 includes a definition/description of "Medium Impact BES Cyber Systems with External Routable Connectivity," that notes an exclusion in the following sentence: "This also excludes Cyber Assets in the BES Cyber System that cannot be directly accessed through External Routable Connectivity." When this definition/description of cyber systems is used for the applicability in requirements such as CIP-006-5 R1.2, R1.4, and R1.5, it is used with the added inclusion of "and their associated…PCA." Looking at the Version 5 definitions document, the definition of Protected Cyber Assets reads "One or more Cyber Assets connected using a routable protocol within or on an Electronic Security Perimeter…" It appears that the inclusive "and associated PCAs" statements in the requirements negates the exclusion statement from the "Background," and makes the intended applicability of such physical security requirements to specific cyber assets unclear for cyber assets without direct external connectivity which reside in the same ESP as cyber assets with direct external connectivity. Requirement 1.5 and 1.7 We would request a change in language that would clarify that the entire BES Cyber Incident Response Team is not required to respond to a Physical Security concern. Suggest the language "Issue an alarm or alert in response to detected unauthorized physical access through a physical access point into a Physical Security Perimeter/to a Physical Control System to appropriate personnel identified in the BES Cyber Security incident Response Plan within 15 minutes of the unauthorized access." CIP-007-5 Requirement 4.4 Recommend changing "undetected" to "potential" Requirement 5.6 Recommend removing "where technically feasible" (If you can't implement technical controls, you can implement procedural controls. The TFE language is not needed.) CIP-008-5 Requirement 1.1 Recommend adding "assess" between "identify" and "classify" Requirement 1.2 Recommend clarifying that only incidents clearly identified as "Reportable Cyber Security Incidents" must be reported to ES-ISAC . Suggest that timeframe specify "Initial notification…exceed one hour from identification as a Reportable Cyber Security Incident." CIP-010-1 Requirement 1.4/1.5 Recommend clarifying when an active test is required. Language in these two requirements is very similar and can be confusing on whether both require an active test or if one requires a review of controls as opposed to testing a change. Requirement 1.5 Recommend the following: Document the results of the testing and, if a test environment was used, the baseline configuration differences between the test environment and the production environment including a description of the measures used to account for any differences in operation between the test and production environments. Where baseline configuration differences are to be documented, the differences must include, at a minimum, the items described in CIP-010: R1.1.1, R1.1.2, R1.1.3, R1.1.4 and 1.1.5. General note: Group expressed concern that three different versions of the standard might be included in one audit. This will create a much more complex audit environment. Entities need one consistent set of standards and clear timeframes for audit periods to reduce the likelihood of multiple standards in one audit.

Group

Western Area Power Administration

Brandy A. Dunn

For CIP-003-5 to 009-5 and CIP-010-1 and 011-1, we agree with the move away from the "zero defects" stance used in Version 3 and 4 standards to the internal controls approach. However, this should have been preceded with an appropriate framework, ample industry involvement, and appropriate outreach and training. We are concerned that NERC is moving forward too quickly without a cohesive strategy by placing language in Standards prior to industry having a complete understanding of (and training on) NERC's definition of "internal controls". Also, the CIP-002-4 and Version-5 "bright-line criteria" steps away from a risk based method to a prescriptive approach. This is an inverted philosophy from the approach Draft-3 used in the other CIP-V5 standards. Although Western appreciates the efforts and reasons behind this, we feel more work will be needed, or perhaps an entirely different approach to Cyber Security in the industry will need to be investigated.

Individual

David Francis

MISO

Comments on CIP Version 5 MISO supports the latest draft of CIP Version 5 as providing greater clarity to Registered Entities regarding their compliance obligations and wishes to commend the SDT for its attention and responsiveness to much of the industry's comments on previous drafts. MISO also supports an overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. In particular, MISO submits that such a shift in focus from strict liability to a regime in which finding and correcting deficiencies is encouraged and in which proactive compliance is rewarded is the only logical way to ensure the security of the Cyber Assets on which the reliable operation of the Bulk Electric System is founded. At the same time, MISO is concerned that the process for determining the sufficiency of a Responsible Entity's efforts to identify, assess, and correct deficiencies is ambiguous and may lead to arbitrary or inconsistent auditing under the regional Compliance Monitoring and Enforcement Programs ("CMEP"). For instance, what constitutes a deficiency may be an issue that is subject to disagreement and varying interpretation. Moreover, the question of whether all deficiencies must be treated equally or whether Entities may implement varying levels and types of responses remains unanswered. Similarly, what constitutes an appropriate corrective measure may also be susceptible to subjective interpretation. With respect to the obligation to identify deficiencies, without further guidance from NERC, it is highly likely that auditors will take inconsistent positions on whether a Responsible Entity's efforts to identify deficiencies were sufficiently robust. Further, without this guidance, an entity is likely to continue to be audited to a strict liability regime with 'consideration' given to its processes to "identify, assess, and correct". This would result in a substantial, additional burden on Registered Entities. Additionally, underlying many of these ambiguities is the question of whether the "identify, assess, and correct" paradigm ostensibly requires the use of internal controls and whether those controls are now subject to audit. Although the September 11, 2012 Webinar specifically states that Version 5 does "not require 'internal controls' or additional process[es]," MISO respectfully submits that the assurance of the SDT on this subject is no guarantee of the verisimilitude of this assertion. More importantly, the structure and substance of an audit of these requirements may well result in a scope that encompasses a Registered Entity's internal controls. Thus, MISO requests that NERC provide, in conjunction with its submission of Version 5 to FERC, public guidance both to the industry and the regional entities containing suggestions for the implementation of "identify, assess, and correct" programs as well as delineating the properly auditable aspects of such programs and the standards that will apply to those aspects in determining compliance. Unless Responsible Entities are able to anticipate – and therefore gear their compliance efforts towards – the proposed auditing of specific aspects of their internal "identify, assess, and correct" programs, these programs will simply extend the industry's current perception of the existing CIP paradigm to the next generation of CIP Reliability Standards, e.g., substantial, administrative burden with minor benefits to the reliability of the Bulk Electric System.
Individual
Rick Keetch
NRG Energy Power Marketing
1. Background –and all standards where language for internal controls state that" each entity shall implement, in a manner that identifies, assesses and corrects deficiencies"- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. 1. CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection." CIP-008 VOTE YES 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include "as applicable". CIP-009 VOTE NO 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center
Individual
Keith Comeaux
NRG Energy, Inc
Individual
Matthew Morais

ERCOT ISO
ERCOT is voting to approve CIP-002-5, but the SDT issued certain guidance statements in response to SRC comments that are potentially problematic in practice. Those matters are discussed below, and ERCOT requests that the SDT take appropriate action consistent with these comments to remedy the potential problems created by the relevant guidance statements. In response to SRC comments that requested clarification on criteria 2.3 and 2.6 with respect to what specifically triggers the relevant third party notifications under those criteria, the SDT noted that with respect to 2.3, the notification is pursuant to a contract – specifically, when the relevant functional entities identify a resource as a Reliability-Must-Run resource. This is potentially problematic. Accordingly, ERCOT requests clarification regarding the appropriateness of using "Reliability Must Run" (RMR) or similar concepts for identifying, "Each generation Facility that its Planning Coordinator or Transmission Planner designates, and informs the Generator Owner or Generator Operator, as necessary to avoid an Adverse Reliability Impact in the planning horizon of more than one year." As an initial matter, RMR contracts are generally only relevant in ISO/RTO markets where they are needed to keep uneconomic units running for reliability purposes until alternative market solutions address the issue. Accordingly, it is questionable if this approach would even be available in vertically integrated regions. In addition, the designation of RMR resources is performed pursuant to specific tariff/protocol processes that are not based on NERC standards, but are rather based on the particular qualifications/conditions in the respective entities rules. As such, it is possible that they are outside of the purview of the NERC Reliability Standards, which are linked to specific reliability standards in Section 215 of the FPA – i.e. the basis for RMR contracts may not align with the basis for the NERC reliability standards. The SDT guidance does refer to the TPL standards and additional contracts generally, but this further confuses the point and creates a disconnect between the relevant processes that drive the notification under criterion 2.3 - RMR contracts are unrelated to the TPL standards or the opaque and undefined process superficially described by the SDT where the RRO coordinates certain actions. Also, because the RMR process is performed by ISOs/RTOs under their tariff rules and not the NERC Standards, they are not executing the agreements in a NERC functional role, which creates a disconnect between the third party NERC functions under criterion 2.3 and the entity executing the RMR with the resource. While it is possible that an ISO/RTO involved in RMR agreements is registered as one of the relevant functions, the function is not making that determination in its NERC functional role (i.e. PC or TP) pursuant to NERC authority. Given the potential problems created by linking the relevant notification to a reliability needs determination pursuant to an RMR process, the SDT should reconsider this guidance as it relates to RMR contracts, and focus on appropriate reliability needs/determinations under relevant NERC Standards, which align with NERC's authority and the reliability metrics that serve as the benchmark for NERC's authority generally and the specific NERC Standards. For example, units may be identified in planning studies performed pursuant to the NERC standards that are not relevant under regions' RMR processes, or vice-versa. Although the SDT discusses TPL-003, the scope of applicable standards under which third party actions trigger notifications pursuant to criterion 2.3 must be specifically defined. The general reference to TPL-003 does not accomplish this. Also, in regards to references to Category C3 contingencies under TPL-003, there is no requirement for the Planning Authority or Transmission Planner to provide or communicate the results of the studies to the asset owners. This would create a new obligation beyond their responsibilities under the NERC Standards. With respect to criterion 2.6, the SRC requested similar clarifications regarding the appropriate scope of standards that trigger the third party notification. The SDT noted that with respect to 2.6, that criterion includes BES Cyber Systems for those Generation Facilities that have been identified as critical to the derivation of IROLs and their associated contingencies, as specified by FAC-014-2, Establish and Communicate System Operating Limits, R5.1.1 and R5.1.3. The SDT went on to note that IROLs may be based on dynamic System phenomena such as instability or voltage collapse, and that derivation of these IROLs and their associated contingencies often considers the effect of generation inertia and AVR response. ERCOT requests clarification as to whether FAC-014-2 is the only standard required for use in identifying, "Generation at a single plant location or Transmission Facilities at a single station or substation location that are identified by its Reliability Coordinator, Planning Coordinator, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies." ERCOT appreciates the specific reference, but in order to provide certainty to all relevant entities, the scope of relevant standards must be specifically defined – the SDT should explicitly state that FAC-014-2 is the only relevant standard, or, alternatively, identify any other relevant standards. It should also be noted that FAC-014-2 does not require the Reliability Coordinator, Planning Coordinator, or Transmission Planner to communicate any of this information to the asset owners. This would create a new obligation beyond their responsibilities under the NERC Standards. CIP-003-5: Requirement R4 requires that an entity have a documented process for identifying and documenting delegations of authority unless there are no delegations. The documentation of the delegation should be sufficient without the need to create and maintain a documented process for identifying and documenting said delegations. This requirement is administrative in nature and is suitable for elimination pursuant to the SAR P81 process. Accordingly, the Standard Drafting Team should consider the need for this requirement in version 5. CIP-004-5: This requirement is administrative in nature and is suitable for elimination pursuant to the SAR P81 process. The risk to the BES would be minimal because a quarterly awareness bulletin was not sent. Accordingly, the Standard Drafting Team should consider the need for this requirement in version 5. Interactive Remote Access Definition: This definition is unworkable in practice. ERCOT is voting to approve the standard to move v-5 forward because it offers incremental improvements over v-4, however, the SDT should provide additional clarification on this interpretation, or revise it, to mitigate the unworkable result of its potential interpretation, which is described below. As written, this definition appears to require that entities declare each of

their internal networks as an ESP, including their corporate networks. Many entities monitor their corporate network in much the same manner as their ESPs. Requiring encryption within their corporate networks would introduce an unacceptable security risk by rendering their monitoring capabilities ineffective. ERCOT requests appropriate clarifications or that the definition be modified to specify that Interactive Remote Access and the associated technical controls be required when traffic is traversing an untrusted or public network only.
ERCOT believes that there are aspects of CIP v-5 that provide incremental benefits relative to v-4. ERCOT supports those aspects of v-5. However, the requirements in v-5 that implicate internal controls are not appropriate for NERC Standards. Accordingly, to support the beneficial aspects of v-5 moving forward, ERCOT is voting in favor of most v-5 standards, subject to the position that the requirements related to internal controls should be removed. Internal controls are not suitable for reliability standards. Entities' internal controls are beyond the scope of Section 215 of the Federal Power Act, and, therefore, beyond the scope of reliability standards. Furthermore, inclusion of internal controls in reliability standards is inconsistent with NERC's risk based initiative because they are not related to actual reliability impacts. In addition, imposition of mandatory controls in reliability standards is inappropriate because of the wide variety of organizational structures, which necessarily requires flexibility with respect to developing appropriate controls for each entity's specific circumstances. Even assuming there was any legitimate basis to include internal controls in reliability standards such requirements would be problematic in practice. The deficiency review processes in the proposed internal controls is ambiguous and susceptible to inefficient and ineffective CMEP results. What constitutes a deficiency will be an issue that is vulnerable to subjective disagreements. Even assuming there is agreement on that issue, what constitutes an appropriate remedy for a deficiency in terms of assessment and correction will similarly be susceptible to subjective disagreements. With respect to the obligation to evaluate the deficiency identification process itself, again, the potential for the introduction of subjective compliance review will be problematic in practice in terms of reviewing the merits of a decision to implement a modification or not, and, if a modification is implemented, whether the revision is adequate. This degree of subjectivity that will necessarily be required for compliance assessments of the relevant requirements is unacceptable. Accordingly, the internal control requirements would be problematic in terms of providing/gathering evidence to demonstrate an adequate level of compliance. In fact the relevant requirements are arguably similar to fill-in-the-blank type standards, which are ideal candidates for elimination pursuant to the SAR P81 effort, which FERC expressly rejected in Order 693 for this exact reason – they lacked adequate and important detail. Furthermore, there are multiple efforts by NERC and the industry related to the appropriate use of internal controls to more effectively administer the CMEP program. For example, the introduction of internal controls into the RSAW documents, the proposed inclusion of internal control requirements into COM-003, and, at issue here, the introduction of such requirements into CIPv5. Against this back drop, it may be best to reconsider the internal controls language in RSAWs and in Standards until such time that NERC and the industry have addressed the concept through the stakeholder process and determined the most effective/efficient means of utilizing internal controls in the relevant NERC programs. Although not appropriate for standards, internal controls can facilitate compliance. As such, the use of internal controls in the CMEP program is appropriate. Entities should receive CMEP benefits for utilizing internal controls. These benefits should be established in the context of CMEP policies/guidelines and/or Rules of Procedure, or, alternatively, considering incorporating such benefits/incentives in non-binding/non-exclusive measures. This use of internal controls is appropriate and should be considered by NERC in concert with industry. However, that approach is completely different than incorporating them in standards, which is inappropriate from both an authority and policy perspective. Consistent with the foregoing discussion, internal controls are inappropriate for reliability standards and v-5 should be revised to remove/revise any requirements that implicate internal controls, whether directly or indirectly. Alternative uses of internal controls in the CMEP program should continue to be reviewed by NERC in appropriate stakeholder forums.
Individual
Kathleen Goodman
ISO New England
Group
Transmission Access Policy Study Group
William J. Gallagher
CIP-002-5, Attachment 1, Section 2.12 now contains minimum thresholds for BA and GOP Control Centers to qualify as Medium Impact. There is no such threshold for TOP Control Centers, however, with the result that no TOP Control Center can be Low Impact. That is not a reasonable result; it is not the case that every TOP Control Center, no matter how small, is at least Medium Impact. TAPS supports the addition of a reasonable threshold to Section 2.12. FMPA's proposal is reasonable and objective: the threshold could be designed like Section 2.5, including >100 kV and <200 kV Facilities with a score of 350; all of the transmission Facilities under the control of the Control Center could be added up and compared to the weighted score 3000 metric of bullet 2.5 to determine if that Control Center is Medium or Low. Alternatively, the decision of whether a TOP Control Center should be considered Medium Impact could be made by the TP or PC, which have the information relevant to make such case-by-case determinations. The starting presumption could be that all non-High Impact TOP Control Centers are Low Impact, or that they are Medium Impact, or that TOP Control Centers that control Transmission Facilities over 200 kV are Medium Impact and those that do not are Low Impact. There are many ways to achieve a reasonable, supportable threshold; failing to include any threshold, however, is not reasonable or supportable. In addition,

TAPS believes that the Applicability section of CIP-002-5 is inconsistent between functional registrations: under Section 4.1.2.4, a DP that owns a Cranking Path is a Responsible Entity, and under Section 4.2.1.4, the standard is applicable to Cranking Paths owned by DPs, without limitation. Under Section 4.2.2, however, the only Elements for which TOs and TOPs must comply – including Cranking Paths - are BES Facilities. Since Cranking Paths are not necessarily BES Facilities under either the current BES definition or the proposed new BES definition, the applicability language in the standard would make non-BES Cranking Paths subject to the CIP standards, but only if owned by DPs. Non-BES Cranking Paths owned or operated by TOs or TOPs would not be subject to the standard. There is no technical justification for this difference. To achieve consistent treatment of DPs, TOs, and TOPs, as well as to take advantage of the work done to develop the proposed new BES definition and BES exception process, TAPS asks the SDT to consider changing the applicability language in Sections 4.1.2.4 and 4.2.1.4 from "Each Cranking Path and group of Elements meeting the initial switching..." to "Each Cranking Path and group of Elements that are part of the BES and that meet the initial switching...."

TAPS supports the SDT's goal of removing the "zero-defect" problem from the CIP standards. We are concerned, however, that use of "shall implement" reintroduces the problem by requiring zero-defect "implementation." We suggest replacing the word "implement" with "institute," so that the evidence required to demonstrate compliance would be, for example, proof of procedures supporting the policy instituted. TAPS suggests, as a general matter of good practice, that the SDT avoid including any requirements that would be likely to be deleted by the Paragraph 81 effort. Data retention requirements (CIP-006-5, R1.9 and R2.3; CIP-007-5, R4.3; and CIP-008-5, R2.3) fall into this category.

Group

Associated Electric Cooperative, Inc. - JRO00088

David Dockery, NERC Reliability Compliance Coordinator

AECI wishes to thank and compliment the SDT for their dedication, effort, and the improved quality of CIP Standards submitted within this third draft for Comment and Ballot, and the SDT's evidenced consideration of earlier comments. AECI is and has recommended to our membership that voting be affirmative for CIP-003-5 through CIP-011-1. Regrettably AECI is voting and recommending negative vote on CIP-002-5. We reference NRECA's comment of concern as well as their proposed wording for revision to CIP-002-5 Attachment 1 Criteria 2.12, and the related new criteria NRECA proposes within the Low Impact (L) section. If the SDT cannot adopt NRECA's proposal, we secondarily propose the SDT's providing an exclusion clause within the Criteria 2.12, for Adverse Impact Studies that determine a TOP to have no Adverse Impact to the BES, consistent with the base criteria within 2.3, yet worded to be exclusive rather than inclusive, and with assurances concerning the quality of such studies before the ERO. Such studies are of course not as simple as a Criteria 2.3 study, yet should be achievable for the class of TOP that AECI envisions exercising the exclusion. AECI is also aware of alternative wording being submitted by APPA, as well as other small entities. We bow to the SDT's expertise on weighing and selecting the most worthy proposal. Without something on the page, AECI does know and is concerned for TOPs that will be wrongfully placed into the Medium Impact Category. Even with this added consideration, CIP Version 5 will provide FERC and NERC with visibility into Low Impact Control Centers, and can then determine whether further governance is warranted. Finally, with added consideration for the smaller TOPs in place, AECI and its members can vote favorably on CIP-002-5 as well.

++CLARITY SUGGESTIONS, Referenced to Clean copies++ (1) For all Requirements including "in a manner that" language to address zero defect, please consider adding the following language to their corresponding Measures: "Where the entity is identifying, assessing, and correcting its own deficiencies, the entity is satisfactorily performing this requirement." (2) Implementation Plan, p 4, final paragraph, QUESTION: Are we to add the time allowances, corresponding with line-item events within the table that immediately follows, to the periodic times for corresponding line-item events? (3) Definitions, Interactive Remote Access, REPLACE: "access may be initiated" WITH: "access is likely initiated" RATIONALE: avoids auditors implying "may only be initiated" (4) Definitions, Protected Cyber Assets ("PCA"), REPLACE: "part" WITH: "a component", REPLACE: "within the same" WITH: "located within or composing a common", REPLACE: "same ESP" WITH: "same ESP (ie High Water Marking)" (5) General, Parts 4.1.2.3 and 4.2.1.3, REPLACE: "is subject to one or more requirements in a NERC or Regional Reliability Standard." WITH: "can affect the reliability of either Medium or High Impact Facilities." RATIONALE: DPs would benefit from additional screening clarity. (6) CIP-002-5 - Attachment 1, part 3 Low Impact Rating (L), Criteria 4.2, REPLACE: "stations" WITH: "Transmission stations" (7) General, "Applicable Systems" Columns in Tables:, bullet "Medium Impact BES Cyber Systems with External Routable Connectivity", COMMENT: "cannot be directly accessed" implies "can be indirectly accessed" so this sentence appears to stray beyond the original SDT intent. (8) CIP-004-5, R4.2 Measures COMMENT: Bottom sentence in R4 Rationale and corresponding Guidelines indicate no SDT expectation that a list of authorizations is necessary, only record of authorizations, but R4.2 becomes less clear because the phrase "list of individuals who have been authorized" appears in both Examples. Could a comparison between quarterly snapshots of provisioned individuals or groups, correlated against chronological record of user authorization changes, serve as an additional Example of the stated intent of this requirement having been met? (9) CIP-004-5, R4.3 Requirement COMMENT: Additional guidance for scope of "specific, associated privileges". Some are concerned auditors might see this as a directive for them to dig-down to individual file-access privileges, although R4 Guidelines appear to bind verification to BES Cyber System access. (10) CIP-004-5, R4.4 Requirement GUIDANCE: Wording of R4.4 appears to preclude Requirements 4.2 and 4.3, for verifying access to information storage locations for BES Cyber System information. Please clarify. ++QUALITY

SUGGESTIONS++ (1) Implementation Plan, p 3, part 6: MOVE: "CIP-006-5, Requirement R3, Part 3.1" to part 7 below, RATIONALE: 24mo periodicity. REMOVE "CIP-008-5, Requirement R3, Part 3.1" and "CIP-009-5, Requirement R3, Part 3.1", RATIONALE: timing conflict with immediate predecessor on list, which triggers timers for these two items. (2) Implementation Plan, p 3, part 7, FYI: Conflicting 36 month periodicity but 24 month initial. (3) Implementation Plan, p 4, Previous Identity Verification, REPLACE: "R4, Part 4.1" WITH: "R3, Part 3.1" (4) General, p 6, Background, (final paragraph supporting 300 MW UVLS/UFLS), MOVE: to CIP-002-5 Guidelines and Technical Basis, REPLACE: with "see CIP-002 Guidelines and Technical Basis"

Individual

Richard Vine

California Independent System Operator

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 for the same rationale as was provided by the Drafting Team in 7.4. A transfer is not as high a risk as a termination.

Individual

Alan Johnson

NRG Energy, Inc.

CIP-003 (Cyber security policies, senior manager and delegation) 1. Background –and all standards where language for internal controls state that" each entity shall implement, in a manner that identifies, assesses and corrects deficiencies"- There is no clear mechanism identified that would explain how this will be interpreted and audited by the regional entity. 2. Requirement R2 should be revised to make it clear that it applies only to low impact BES cyber systems (it is inconvenient to have to refer back to the CIP-002 R2 and this is not consistent with the wording of R1). 3. Requirement 4- If a delegate can delegate authority to another person (as contemplated in the Guidelines and Technical Basis section), that should be made clear in the requirement itself. CIP-004 1. CIP-004-5 R2.1 contains elements which can comprise a training program. If role-based training is required (as indicated by R. 2), must all roles identified receive some training from each of the elements in R2.1? If all roles must receive some training for each of the elements in R. 2.1, what is the value of having role-based training? Customized training per roles- how many would be required? This would be difficult to identify, coordinate, implement and measure. Please provide detail as to role definition. Define if training is classified at high level description of user roles or defined by various tasks to determine training. CIP-006 VOTE YES 1. Requirement 1.7 should be revised from "within 15 minutes of the unauthorized physical access." to "within 15 minutes of detection." CIP-008 1. Requirement 3.1.2- implies that the Cyber Security Incident Response plan must be updated based on any documented lessons learned. However, lessons learned may not impact any change in the plan but relate to execution of the plan and performance of the personnel in that execution. This should be reworded to include "as applicable". CIP-009 1. Although best practice, through implementation of activities as outlined in Requirement R1.5, this can result in significant impact to the BES as this can result in considerable delay to return to service following a actual recovery, particularly in a control center. DEFINITION: Control Center- as data centers are not a defined term, an entity should be able to choose what constitutes as an associated data center

Individual

Dale Dunckel

OCPD

Sections 4.1.2.1 and further 4.2.1.1 and Section 4.1.2.3 it appears in these section that a small entity that has a stand alone UFLS system with no communication is subject to a cyber security standard. Further a small entity that is part of a larger load shedding program should maintain their program, but the entity that is responsible should be the one with the cyber security based on the common control system.

Group

Hydro One

Sasa Maljukan

– To avoid possible confusion and misinterpretation we suggest changing "at least once every 15 calendar months" to "at least once in every 15 calendar months period." – For clarification, suggest adding "mimic display" to the second paragraph of CIP-007 R5 Rationale, resulting in "Interactive user access does not include read-only information access in which the configuration of the Cyber Asset cannot change (e.g. front panel displays, web-based reports, mimic displays etc.)." – CIP-008 R1 Part 1.2 requires reporting to the ES-ISAC which may not be acceptable to the Canadian entities. We'd like to suggest that the current wording is replaced with more general one. – We recommend changing CIP-008 R2 Part 2.1 from "at least once every calendar year, not to exceed 15 months" to "at least once in every 15 calendar months period." – For clarity, recommend changing CIP-009 R1 Part 1.5 from "One or more processes to preserve data for determining the cause of a Cyber Security Incident that

triggers activation of the recovery plan(s), per device capability. Data preservation should not impede or restrict recovery" to "One or more processes, per device capability, to preserve data for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s), except where data preservation impedes or restricts recovery."

Individual

Rebecca Moore Darrah

MISO

MISO supports the latest draft of CIP Version 5 as providing greater clarity to Registered Entities regarding their compliance obligations and wishes to commend the SDT for its attention and responsiveness to much of the industry's comments on previous drafts. MISO also supports an overall shift in the emphasis of compliance from perfection to the identification, assessment, and correction of deficiencies. In particular, MISO submits that such a shift in focus from strict liability to a regime in which finding and correcting deficiencies is encouraged and in which proactive compliance is rewarded is the only logical way to ensure the security of the Cyber Assets on which the reliable operation of the Bulk Electric System is founded. At the same time, MISO is concerned that the process for determining the sufficiency of a Responsible Entity's efforts to identify, assess, and correct deficiencies is ambiguous and may lead to arbitrary or inconsistent auditing under the regional Compliance Monitoring and Enforcement Programs ("CMEP"). For instance, what constitutes a deficiency may be an issue that is subject to disagreement and varying interpretation. Moreover, the question of whether all deficiencies must be treated equally or whether Entities may implement varying levels and types of responses remains unanswered. Similarly, what constitutes an appropriate corrective measure may also be susceptible to subjective interpretation. With respect to the obligation to identify deficiencies, without further guidance from NERC, it is highly likely that auditors will take inconsistent positions on whether a Responsible Entity's efforts to identify deficiencies were sufficiently robust. Further, without this guidance, an entity is likely to continue to be audited to a strict liability regime with 'consideration' given to its processes to "identify, assess, and correct". This would result in a substantial, additional burden on Registered Entities. Additionally, underlying many of these ambiguities is the question of whether the "identify, assess, and correct" paradigm ostensibly requires the use of internal controls and whether those controls are now subject to audit. Although the September 11, 2012 Webinar specifically states that Version 5 does "not require 'internal controls' or additional process[es]," MISO respectfully submits that the assurance of the SDT on this subject is no guarantee of the verisimilitude of this assertion. More importantly, the structure and substance of an audit of these requirements may well result in a scope that encompasses a Registered Entity's internal controls. Thus, MISO requests that NERC provide, in conjunction with its submission of Version 5 to FERC, public guidance both to the industry and the regional entities containing suggestions for the implementation of "identify, assess, and correct" programs as well as delineating the properly auditable aspects of such programs and the standards that will apply to those aspects in determining compliance. Unless Responsible Entities are able to anticipate – and therefore gear their compliance efforts towards – the proposed auditing of specific aspects of their internal "identify, assess, and correct" programs, these programs will simply extend the industry's current perception of the existing CIP paradigm to the next generation of CIP Reliability Standards, e.g., substantial, administrative burden with minor benefits to the reliability of the Bulk Electric System.