

## Unofficial Comment Form for Project 2008-06 — Cyber Security Order 706 Draft CIP-002-4 Informal Review

Please **DO NOT** use this form to submit comments. Please use the [electronic form](#) located at the link below to submit comments on the proposed CIP-002-4. Comments must be submitted by **June 3, 2010**. If you have questions please contact Joe Bucciero at [joe.bucciero@gmail.com](mailto:joe.bucciero@gmail.com) or by telephone at (267) 981-5445.

[http://www.nerc.com/filez/standards/Project\\_2008-06\\_Cyber\\_Security\\_PhaseII\\_Standards.html](http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security_PhaseII_Standards.html)

### Background Information:

[FERC Order 706](#) directed NERC to develop modifications to the CIP Reliability Standards on Cyber Security. Some of the modifications were straightforward. Other Order 706 changes, such as modification to the scope of assets covered by the standard and consideration of the NIST framework, are more complex and required additional consideration. A Standards Drafting Team (SDT) was appointed by the Standards Committee on August 7, 2008 to develop these revisions as part of Project 2008-06 — Cyber Security Order 706. The SDT has been assigned the responsibility to review each of the CIP reliability standards to ensure that they conform to the latest version of the [ERO Rules of Procedure](#), including the [Reliability Standards Development Procedure](#), and also address all of the directed modifications identified in the FERC Order 706.

Due to the large number of changes, some of which are complex issues, directed in Order 706 and the complexity of the project, the SDT adopted a multi-phase strategy to revise the CIP standards. The initial phase of the project modified the CIP standards (CIP-002-1 through CIP-009-1) to comply with the near term specific directives included in FERC Order 706. The SDT's work in this initial phase resulted in Version 2 of the CIP standards. On September 30, 2009 FERC approved Version 2 of the CIP standards with an effective date of April 1, 2010.

In its [September 30 Order](#), FERC directed NERC to make additional changes to two of the CIP standards (CIP-006-2 and CIP-008-2) and the associated implementation plan. Although FERC directed changes to only two of the eight (CIP-002-2 thru CIP-009-2) CIP standards, conforming changes were drafted for the remaining six CIP standards (CIP-002-2 through CIP-005-2, CIP-007-2, and CIP-009-2) to correct the cross references within the set of standards. The output of this work became Version 3 of the CIP standards. Version 3 of the CIP standards (CIP-002-3 to CIP-009-3) was approved by FERC on March 31, 2010 and become effective on October 1, 2010.

The SDT is currently developing changes to the CIP reliability standards to address the Order 706 directives that require significant industry debate.

In December 2009, the SDT posted an initial draft of the first CIP cyber security reliability standard (CIP-002-4 — Cyber Security — BES Cyber System Identification and Categorization) for a 45 day informal comment period. The SDT received more than 500 pages of comments from industry stakeholders. The SDT reviewed each of the comments received from the stakeholders, and considered their scope and direction throughout the development of the revised draft of the CIP standard. Subsequent to this initial posting, and in consideration of the significant change in scope for the revised CIP standard, the

drafting team has changed the designation of the first CIP reliability standard to CIP-010-1 — Cyber Security — BES Cyber System Categorization.

At its meeting on April 13–16, 2010, the SDT agreed on category headings for use in the posting and using a table approach for determining applicability. The SDT also agreed that, due to the nature of the proposed changes to the existing CIP standards, the best course of action would be to retire the existing standards and start a new sequence, starting with CIP-010 for the BES Cyber Asset Categorization. The SDT agreed to go forward with one standard (CIP-011) for all of the control requirements for the informal posting, asking for industry input on the comment form on the two format approaches considered.

In response to comments received from a large number of entities to post the requirements for categorization of BES Cyber Systems together with the requirements for the application of controls, the SDT has modified its schedule and intends to ballot the CIP standards as a single package. In consideration of the very different approach, model and format used in the drafting of these new CIP standards, the SDT is proposing a set of two standards in lieu of the original eight standards in the CIP series: CIP-010-1 establishes the foundation for cyber security protection by requiring the identification of what to protect and their categorization; CIP-011-1 establishes baseline cyber security requirements, which must be applied to protect the BES Cyber Systems identified and categorized in CIP 010-1 according their impact category. The alternate format would include CIP-010-1 as described above but would group the baseline cyber security requirements in multiple separate standards numbered consecutively as CIP-011-1, CIP-012-1, CIP-013-1, and so on. In the drafting these standards, the SDT considered CIP standards Version 1, 2, and 3 directives from FERC Order 706, FERC approved Interpretations to the CIP Version 1 requirements, and other cyber security standards such as NIST 800-53 and the DHS Catalog of Control Systems Security.

### **Implementation Plan Considerations**

The SDT is currently developing an Implementation Plan for these standards which will consider the following:

1. BES Cyber Systems categorized as High Impact which were previously designated as Critical Cyber Assets;
2. BES Cyber Systems categorized as High Impact which were NOT previously designated as Critical Cyber Assets;
3. BES Cyber Systems categorized as Medium Impact which were previously designated as Critical Cyber Assets;
4. BES Cyber Systems categorized as Medium Impact which were NOT previously designated as Critical Cyber Assets;
5. BES Cyber Systems categorized as Low Impact which were previously designated as Critical Cyber Assets;
6. BES Cyber Systems categorized as Low Impact which were NOT previously designated as Critical Cyber Assets;
7. New requirements not previously included in the CIP Version 1,2, and 3 standards, as they relate to the above categories;
8. Re-categorized BES Cyber Systems;
9. Nuclear Facilities.

The Implementation Plan will be posted as part of the future posting package for formal comments.

The Cyber Security Order 706 Standard Drafting Team requests industry feedback on the initial draft of CIP-010-1 — Cyber Security — BES Cyber System Categorization and of CIP-011-1 — Cyber Security — BES Cyber System Protection. In addition, the SDT is requesting feedback from the industry on whether they prefer the currently proposed format for CIP-011-1, which contains a complete set of requirements; or an alternate format, where the requirements are grouped in separate standards. Industry feedback gathered will be utilized by the drafting team to refine the draft standard for formal industry review in July/August 2010.

**\*Please use the [electronic comment form](#) to submit your final responses to NERC.**

**Questions:**

1. Do you agree with the adoption of the following new or revised terms and their definitions for inclusion in the NERC Glossary: BES Cyber System Component, BES Cyber System, and Control Center? If not, please explain and supply your proposed modification.

**1.a. BES Cyber System Component** — One or more programmable electronic devices (including hardware, software and data) organized for the collection, storage, processing, maintenance, use, sharing, communication, disposition, or display of data; which respond to a BES condition or Disturbance; or enable control and operation.

- Agree with proposed definition  
 Disagree with proposed definition

Comments: We think the existing definition is too broad and propose the following: One or more programmable electronic devices (including hardware and software) organized to enable control, operation and protection of BES equipment.

**1.b. BES Cyber System** — One or more BES Cyber System Components which if rendered unavailable, degraded, compromised, or misused could, within 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES, or affect situational awareness of the BES.

- Agree with proposed definition  
 Disagree with proposed definition

Comments:

We feel "affect situational awareness of the BES" should be removed, as this is already covered under "operation of the BES". As written, situational awareness is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for operation of the BES.

We also feel "misused" should be removed, as this is already covered under "compromised".

As currently worded, we also believe the intent of the 15 minute time frame is ambiguous. We would propose incorporating what we believe to be the drafting team's true intent directly in to the definition, along with our other suggestions, as follows:

One or more BES Cyber System Components which if rendered unavailable, degraded, or compromised could, within an operational time horizon of 15 minutes, cause a Disturbance to the BES, or restrict control and operation of the BES.

**1.c. Control Center** — A set of one or more BES Cyber Systems capable of performing one or more of the following functions for multiple (i.e., two or more) BES generation Facilities or Transmission Facilities, at multiple (i.e., two or more) locations:

- Supervisory control of BES assets, including generation plants, transmission facilities, substations, Automatic Generation Control systems or automatic load-shedding systems,

- Acquisition, aggregation, processing, inter-utility exchange, or display of BES reliability or operability data for the support of real-time operations,
- BES and system status monitoring and processing for reliability and asset management purposes (e.g., providing information used by Responsible Entities to make real-time operational decisions regarding reliability and operability of the BES),
- Alarm monitoring and processing specific to operation and restoration function, or
- Coordination of BES restoration activities.

Agree with proposed definition

Disagree with proposed definition

Comments:

2. The definition of BES Cyber System limits the scope of the definition and the applicability of CIP-010-1 (and CIP-011-1) to real-time operations systems with an operational time horizon of 15 minutes. Do you agree with this scope of applicability? If not, please explain why and provide specific suggestions for improvement.

Agree with scope

Disagree with scope

Comments:

3. Requirement R1 of draft CIP-010-1 states, "Each Responsible Entity shall identify and document each of the BES Cyber Systems that it owns to execute or enable one or more functions defined in CIP-010 – 1 Attachment I – Functions Essential to the Reliable Operation of the BES to identify BES Cyber Systems for the application of security requirements." Do you agree with the proposed Requirement R1? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments: We feel R1 is ambiguous as written when referring to assets of joint ownership, and would propose replacing the word "owns" with "owns and operates". As currently written, this requirement would force each owner to individually catalogue all of the BES Cyber Systems at a jointly owned facility, even though typically only the actual operator of the facility has anything to do with the BES Cyber Systems installed, or the related day-to-day compliance with NERC standards.

4. Requirement R2 of draft CIP-010-1 states, "Each Responsible Entity shall categorize and document such categorization for each BES Cyber System identified in Requirement R1 according to the criteria contained in CIP-010-1 Attachment II – Impact Categorization of BES Cyber Systems to categorize the BES Cyber Systems identified in Requirement R1 for the application of Cyber Security requirements commensurate with the potential impact on the BES." Do you agree with the proposed Requirement R2? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments:

5. Requirement R3 of draft CIP-010-1 states, "To ensure the application of adequate requirements on its BES Cyber Systems, each Responsible Entity shall:
- 3.1 review the identification and categorization of its BES Cyber Systems within 36 months of the last identification and categorization
  - 3.2 review the identification and categorization of its BES Cyber Systems as a result of any planned change to the portion of the BES that it owns
  - 3.3 update, when applicable, the documentation specified in Requirements R1 and R2 within 45 calendar days of the completion of such change to the BES."

Do you agree with the proposed Requirement R3? If not, please explain why and provide specific suggestions for improvement.

- Agree  
 Disagree

Comments: For item 3.2, we believe the word "planned" should be replaced with "incorporated". Otherwise, an entity could end up identifying and categorizing BES Cyber Systems that never actually end up getting installed.

6. CIP-010-1 Attachment I contains a listing and brief description of Functions Essential to Reliable Operation of the Bulk Electric System. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

- Yes  
 No

Comments: We propose to remove "monitoring" from the Monitoring and Control function. As written, the term "monitoring" is so ambiguous that any meter, instrument, transducer, etc. could possibly be interpreted as included, even if these devices are not required for control of the BES.

We would propose using the following:

Control – Activities, actions and conditions that provide control of BES elements.

7. CIP-010-1 Attachment II contains criteria for categorization of BES Cyber Systems for High, Medium and Low impact categories. The criteria were originally developed in collaboration with representatives of the Operating and Planning Committees, some of whom continued to provide input during the drafting of Attachment II. Do you have any suggestions that would improve the proposed criteria? If so, please explain and provide specific suggestions for improvement.

- Yes  
 No

Comments:

Item 1.3

We believe this item may be problematic in nature, as the designation of reliability "must run" units is something that could fluctuate. This would create administrative difficulties for an entity and their RTO as a unit moves between Impact Ratings. We believe this item

needs further clarification to indicate its true intent, such as who stipulates the “must run” designation, what constitutes “reliability must run”, etc.

#### Item 1.4

Item 1.4 uniformly identifies all BES Cyber Systems associated with a Generation Facility designated as a Blackstart Resource in the Transmission Operator’s restoration plan as having a High Impact Rating with regards to the Bulk Electric System. Albeit on a smaller scale, this appears to be the same “one size fits all” approach of the current standards that the SDT is working so diligently to address. In reality, all Blackstart Resources do not carry the same importance to even the utility itself, let alone to the Bulk Electric System. Therefore, we believe there should be a hierarchy for Blackstart Resources, similar to nearly all other elements being considered, categorizing their associated BES Cyber Systems as High, Medium, or Low Impact.

To implement this approach, we believe it is imperative to consider the Blackstart Resource’s actual role in the restoration plan, not just its simple inclusion. A 10 MW Blackstart Resource that directly supports restoration of a large generating facility is much more important to the Bulk Electric System than a 10 MW Blackstart Resource that simply supplies localized load during an outage. Therefore, we would propose judging the relative importance of a Blackstart Resource by the relative importance of the facilities it directly supports.

We would recommend rewording item 1.4 as follows, leveraging the existing language of Item 1.8:

“Generation Facilities designated as Blackstart Resources in the Transmission Operator’s restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.”

We believe this approach should provide a better sense of a facility’s true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

#### Item 1.5

We need to clarify the meaning of “Transmission lines”. If a 300 kV substation has a terminal connected to a 345/115 kV transformer, which then feeds a 115 kV transmission line leaving the facility, does this constitute a 115 kV or 345 kV “Transmission line” within the context of this item? For this example, we would interpret this to be a 115 kV line, so it would not be included in the Transmission line count for the substation bright line.

We also believe the bright line should take higher voltages in to consideration. A substation with three 765 kV lines would not be High Impact, but a substation with four 345 kV lines would be. We propose additional criteria of two or more 500 kV lines, or simply adding to/changing the High Impact criteria along the lines of the Medium Impact criteria (item 2.6), calling out “Transmission Facilities operated at 500 kV or higher...”

#### Item 1.6

We would recommend rewording item 1.6 as follows for consistency in approach with the proposed Item 1.4:

“Facilities required by the Transmission Operator’s restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 1.1 above.”

We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

**Item 1.14**

We would recommend rewording item 1.14 as follows:

"Transmission Operator functions performed by primary or backup Control Centers that remotely control two or more BES Cyber Systems with a Medium Impact Rating, or one or more BES Cyber Systems with a High Impact Rating."

We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System.

**Item 2.7**

We would recommend rewording item 2.7 as follows:

"Transmission Operator functions performed by primary or backup Control Centers that remotely control one or more BES Cyber Systems with a Medium Impact Rating, not included in Section 1."

We believe this approach should provide a better sense of a control center's true impact on the Bulk Electric System.

**Section 2 Additions**

We would recommend adding the following items under section 2, Medium Impact Rating, for consistency in approach with the proposed Items 1.4 and 1.6:

- "Generation Facilities designated as Blackstart Resources in the Transmission Operator's restoration plan that directly support the start up of a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."
- "Facilities required by the Transmission Operator's restoration plan to directly support a primary Cranking Path for a Generation Facility with aggregate rated capabilities as described in Part 2.1 above, not included in Section 1."

We believe this approach should provide a better sense of a facility's true impact on the Bulk Electric System, resulting in High, Medium, and Low Impact Ratings that adequately address system reliability in a practical manner.

8. Do you have any other comments to improve this version of draft standard CIP-010-1? If so, please explain and provide specific suggestions for improvement.

Comments:

**Questions — CIP-011-1 — Cyber Security — BES BES Cyber System Protection:**

CIP-011-1 is a combination of CIP-003-3 through CIP-009-3 plus additional requirements based on FERC Order 706. The drafting team is proposing to retire the existing CIP-003-3 through CIP-009-3 standards once CIP-011-1 is adopted. This is the first time that CIP-011-1 has been posted for informal industry comment.

9. Do you prefer the currently proposed format for CIP-011-1, which contains a complete single set of requirements? Do you prefer the alternate format, where the requirements are grouped in separate standards? Or do you have no preference?

- Keep CIP-011-1 as one document
- Break CIP-011-1 up into multiple standards

No preference

Comments:

10. The Purpose of draft CIP-011-1 states, "To ensure Functional Entities develop cyber security policies and apply necessary cyber security protection to the BES Cyber Systems for which they are responsible and that execute or enable functions essential to reliable operation of the interconnected BES." Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments:

**Security Governance and Policy (R1)**

11. Requirement R1 of draft CIP-011-1 states, "Each Responsible Entity shall develop, implement, and annually review formal, documented cyber security policies that address the following for its BES Cyber Systems:" and then provides a list of topics that must be addressed. Do you agree with this proposal and list? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments:

**Personnel Training, Awareness, and Risk Assessment (R2 – R4)**

12. Requirements R2 to R4 of draft CIP-011-1 concern personnel training, awareness, and risk assessment, which were previously contained in CIP-004. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

Agree

Disagree

Comments: We would propose replacing the terms "provide all" with "make available to all", as we are concerned the word "provide" could be interpreted to include documenting that the materials were actually received by all personnel. For example, it would be very difficult to document that bulletin board postings were "provided" to each individual employee.

13. Do you agree with the proposed definitions for external connectivity, routable protocol, and non-routable protocol? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments:

14. Tables R3 and R4 provide direction concerning what impact level of BES Cyber Systems to which Requirements R3 and R4 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments:

For item 3.1 and 3.2, we propose making the Low Impact criteria "Required". Cyber Security Training is something that should probably be carried out across the BES.

For item 3.2, we would propose removing "with routable external connectivity", and then adding the following under Medium Impact: "Required for routable external connectivity only".

For item 4.2, we would propose removing "with routable external connectivity", and then adding the following under Medium Impact: "Required for routable external connectivity only".

If an entity is required to restrict physical access, then they should also be required to provide training.

### **Physical Security (R5 – R6)**

15. Requirements R5 and R6 of draft CIP-011-1 concern procedures for physical security, which were previously contained in CIP-006. Do you agree with this proposal? If not, please explain why and provide specific suggestions for improvement.

- Agree  
 Disagree

16. Tables R5 and R6 provide direction concerning what impact level of BES Cyber Systems to which Requirements R5 and R6 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments:

For item 5.1, we propose making the Low Impact and Medium Impact criteria "Required". Restricting physical access is something that should, and is probably already, being carried out almost everywhere in the BES. Physical security is one of the first lines of defense for all facilities, but the most important defense for those facilities without routable external connectivity.

For item 5.2 through 5.11, we would propose adding the following under Medium Impact: "Required for routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability. This approach builds consistency within R5 and R6.

Item 5.3 requires entities to "log" access, and item 5.4 requires entities to "log (manual or automated)" access. Either item 5.3 should define the scope of "logging"

access, or “manual or automated” should be deleted from item 5.4 because “log” by itself could already indicate either manual or automated processes.

For item 5.7, since termination with cause could occur without warning, revoking access within 24 hours may not be practical at distributed locations without routable external connections, where changes may need to be implemented locally. We would propose including a longer timeline for areas without routable external connections. We also believe a two tiered approach would be practical, where personnel specific access devices (manual keys, key cards, etc.) are removed immediately, and then wide scale access changes (shared combination locks, etc.) are allowed more time to be addressed. We believe this approach is similar to that of the NRC.

For items 6.1 – 6.3, we would propose all Medium Impact criteria to be changed to “Required for routable external connectivity only”, to maintain consistency with existing wording within the standard.

For items 6.1 – 6.3, the drafting team may want to consider how these requirements apply to areas without any type of automated physical access control system. What if access is simply restricted by keys, manual logging, and door alarms transmitted by the local RTU to a Control Center? This approach would appear to meet the requirements of R5, but would not seem to be applicable to the requirements of R6.

#### Electronic Access Control (R7 – R14)

17. Requirement R7 of draft CIP-011-1 states “Each Responsible Entity shall document BES Cyber System accounts by incorporating the criteria specified in CIP-011-1 Table R7 – Account Management Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.” Do you agree with the list of electronic access control requirements that are included in Requirements table R7? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please Explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments: Many types of equipment found in generating facilities or substations do not have typical “accounts”, although they may have some type of access control (configuration password). To alleviate this, we propose adding the following to the end of R7: “Required for only BES Cyber System Components with account management capabilities.” Without this addition, we believe this item sets the stage for numerous TFE’s within the industry.

18. Table R7 provides direction concerning what impact level of BES Cyber Systems to which Requirement R7 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments: We agree, assuming the suggested statement under question 17 is included.

19. At the present time, the Access Control requirements for Physical Access have not been combined with the Access Control requirements related to Electronic Access. Do you

agree with this method? Or would you prefer to have the Physical Access control requirements combined with the Electronic Access control requirements? Please explain and provide any suggestions for modification.

- Agree with proposed method
- Combine Access Control requirements

Comments:

20. Requirement R8 of draft CIP-011-1 states “Each Responsible Entity shall apply the criteria specified in CIP-011-1 Table R8 – Account Management Implementation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.” Do you agree with the list of criteria that are included in Requirements Table R8? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each criteria as represented in the table? Please explain and provide any suggestions for modification.

- Agree
- Disagree

Comments: Note impact level comments under question 21.

21. Table R8 provides direction concerning what impact level of BES Cyber Systems to which Requirement R8 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree
- Disagree

Comments: For item 8.1 through 8.3, we would propose adding the following under Medium Impact: “Required for routable external connectivity only”. We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.

22. FERC has mandated immediate revocation of access privileges when an employee, contractor or vendor no longer performs a function that requires physical or electronic access to a critical cyber asset. Requirement R9 of draft CIP-011-1 states “Each Responsible Entity shall revoke system access to its BES Cyber Systems as specified in CIP-011-1 Table R9 – Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.” Do you agree with the list of criteria that are included in Requirements Table R9? Please explain and provide any suggestions for modification, including time proposals. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

- Agree
- Disagree

Comments: If physical access is removed per R5, and remote access is removed per R13, this effectively removes all avenues to electronic access. Therefore, we propose that the period for removing electronic access be lengthened.

23. Table R9 provides direction concerning what impact level of BES Cyber Systems to which Requirement R9 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments: For item 9.1 through 9.4, we would propose adding the following under Medium Impact: "Required for remote access or routable external connectivity only". We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.

For item 9.1, we believe the Low Impact requirement should be deleted, to maintain consistency with R5.7 (revoking physical access for cause) and R8.1 (authorizing electronic access).

24. Requirement R10 of draft CIP-011-1 states "Each Responsible Entity shall implement the account management access control actions specified in CIP-011-1 Table R10 – Account Access Control Specifications to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems." Do you agree with the list of criteria that are included in Requirements Table R10? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments:

We believe the depth of detail in R10 needs to be better coordinated with the rest of the standard, where the entity is told what they need to do, not explicitly how to do it. R10 appears to be overly prescriptive, which could potentially box entities in if they want to exceed the requirements of the standard.

We would propose replacing item 10.1 with something more generic, like "Restrict electronic access to BES Cyber Systems", similar to how physical access is handled under R5.1. Passwords may not apply in all cases, and some entities may wish to implement alternative methods of user authentication that are superior, but as currently worded they would be limited by the standard.

We would also propose replacing item 10.2 with something more generic, like "Electronic access controls shall be reviewed at least once every 12 months". A requirement for changing the access controls every 12 months is not applicable for an entity using biometrics scanning as opposed to passwords.

Finally, we would propose deleting items 10.3 – 10.5, as they would not apply under the approach proposed here.

25. Table R10 provides direction concerning what impact level of BES Cyber Systems to which Requirement R10 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments: With the changes proposed in question 24, we would propose that revised items 10.1 and 10.2 be "Required" for Low, Medium, and High Impacts.

We would agree with the current impact levels for items 10.6 – 10.8.

However, if the standard were to remain as written, we would propose that the 10.1 – 10.3 requirements be removed for Low Impact systems, and be "Required for remote access or routable external connectivity only" for Medium Impact systems. Once someone has gained physical access to a facility, the hurdle of a password does very little to limit the amount of physical damage or misuse that can be done. However, for remote access, the password becomes critical to preventing damage or misuse. We also believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.

26. Requirement R11 of draft CIP-011-1 states "Each Responsible Entity that allows remote or wireless electronic access to any of its BES Cyber Systems shall apply the criteria specified in CIP-011-1 Table R11– Wireless and Remote Electronic Access Documentation to ensure that no unauthorized access is allowed to its BES Cyber Systems. Do you agree with the list of criteria that are included in Requirements Table R11? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments:

27. Do you agree with the definition of remote access as proposed for this standard? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments: As written, the definition could be interpreted to include simple data exchanges between an RTU and a SCADA master, although we do not believe this was the intent of the drafting team. We would propose adding the following to the end of the existing definition: "Automated data exchange systems would not be considered remote access".

28. Table R11 provides direction concerning what impact level of BES Cyber Systems to which Requirement R11 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments: For items 11.2 and 11.3, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.

29. Requirement R12 of draft CIP-011-1 states “Each Responsible Entity that allows wireless and remote electronic access to any of its BES Cyber Systems shall manage that electronic access in accordance with the criteria specified in CIP-011-1 Table R12 – Wireless and Remote Electronic Access Management to ensure that no unauthorized access is allowed to its BES Cyber System.” Do you agree with the list of criteria that is included in Requirements Table R12? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification. Do you agree with the impact levels for each item as represented in the table? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments: Note impact level comments under question 30.

30. Table R12 provides direction concerning what impact level of BES Cyber Systems to which Requirement R12 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Agree

Disagree

Comments: For item 12.1, given the definitions provided in the standard, how can you have remote access without external connectivity? Both terms as defined seem to represent communications between a BES Cyber System and a device external to the BES Cyber System.

31. Requirement R13 of draft CIP-011-1 states “Each Responsible Entity shall revoke remote access by disabling one or more of the multiple factors required for such remote access to BES Cyber Systems by implementing the criteria requirements specified in CIP-011-1 Table R13 – Remote Access Revocation to prevent malicious operation of BES Elements by maintaining control of access to its BES Cyber Systems.” Do you agree with the list of criteria that is included in Requirements Table R13? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments:

32. Table R13 provides direction concerning what impact level of BES Cyber Systems to which Requirement R13 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Agree

Disagree

Comments: As written, we believe the timelines specified for the High Impact criteria are not practical. The tight requirements seem to set up the entire industry for non-compliance, especially with regards to control centers where revocation must occur within one hour. We propose timelines that are more consistent with R5 (physical access) and R9 (electronic access), but would be in agreement with terminology urging entities to expedite this process as much as possible with regards to remote access.

33. Requirement R14 of draft CIP-011-1 states “Each Responsible Entity shall document and implement its organizational processes, technical mechanisms, and procedures for control of wireless and remote access to electronic access points to its BES Cyber Systems including wireless and remote access if it is used, that incorporate the criteria specified in CIP-011-1 Table R14 – Wireless and Remote Electronic Access Controls to ensure that no unauthorized access is allowed to its BES Cyber Systems.” Do you agree with the list of criteria that is included in Requirements Table R14? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments:

34. Table R14 provides direction concerning what impact level of BES Cyber Systems to which Requirement R14 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments: We believe items 14.3 and 14.4 are going to set the stage for numerous TFE's within the industry. Many devices (i.e., protective relays) do not support explicit access permissions and appropriate use banners.

### **System Security (R15 – R19)**

35. Requirements R15 to R19 of draft CIP-011-1 concern procedures for system security protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R15 to R19? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments: As written, item 17.2 does not appear to be applicable to many BES Cyber System Components. Many devices do not allow for disabling ports via software settings, requiring an entity to either file a TFE, or physically disable the ports, resulting in voided warranties for new equipment. Plus, if all of the BES Cyber System Components are already within a physically secure area (per the standards), is disabling ports really necessary? We believe this item should be deleted.

As written, item 19.2 could be interpreted to include all of the RTU communications back to the SCADA master within the control center. We believe it may be impractical to evaluate all data of this type marked as potentially invalid (i.e., out of

range alarms, bad scan alarms, etc.), and to prove it was not compromised maliciously.

36. Tables R15 to R19 provide direction concerning what impact level of BES Cyber Systems to which Requirements R15 to R16 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Agree

Disagree

Comments: For items 15.1 – 15.3, 16.1 – 16.2, and 17.1 we would propose using the following under Medium Impact and High Impact: “Required for routable external connectivity only”. We believe this makes an important distinction between protecting just the BES Cyber System in question, or protecting all other BES Cyber Systems that may be externally connected to it via routable connections, where there would be a real threat of a propagating attack/vulnerability.

We believe the time frames for item 18.4 may not be practical at distributed locations without routable external connections, where logs would need to be reviewed locally.

### Boundary Protection (R20 – R22)

37. Requirements R20 to R22 of draft CIP-011-1 concern procedures for boundary protection. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R20 to R22? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments:

We believe item 20.2 is going to set the stage for numerous TFE’s within the industry. Many devices (i.e., protective relays) do not support explicitly authorized communication.

We believe item 20.4 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.

We believe item 20.5 should specify “at each electronic access point established in Part 20.2”, similar to item 20.3. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only.

We believe the following should be added to the end of item 20.6: “at each electronic access point established in Part 20.2”. This item does not appear to be applicable for non-routable connections, and adding this language would assure it is limited to routable and dialup connections only. It also makes for a consistent approach with item 20.3.

Items 21.1 and 21.2 use the term Cyber System Components, which is undefined. This term either needs to be defined, or replaced with BES Cyber System Components.

Item 21.2 requires that all external communications flow through an electronic access point as established in R20. However, R20.2 only establishes electronic access points for routable and dialup connections. If an entity employs non-routable connections, these would not be defined under R20.2, and thus R21.2 would not allow the entity to communicate through them. We believe item 21.2 should just be deleted, as it seems to add nothing to the standard.

38. Do you agree with the proposed definition of electronic access point? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments:

39. Tables R20 to R22 provide direction concerning what impact level of BES Cyber Systems to which Requirements R20 to R22 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Agree

Disagree

Comments: For items 20.4 – 20.6, we believe “for external connectivity only” should be removed from the impact levels to properly coordinate with the comments on these items made under question 37.

### Configuration Change Management (R23)

40. The configuration change management requirement is centered on the identification of a component inventory and baseline configuration. Do you agree with the list of criteria that are included in the baseline configuration? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the baseline and managed through the configuration change management process? Do you agree with the list of criteria that are included in Requirements Table R23? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in Table R23? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments: This requirement, especially evident in item 23.2, appears to be written around typical IT equipment, and not the multitude of electronic programmable devices an entity will encounter in the field at a generating facility or substation. Therefore, we believe the current intent of this requirement should only apply to control centers, similar to item 23.6, where typical IT equipment is becoming more of the standard.

For generating facilities and substations, we believe it would be adequate to require the entity to document and implement one or more processes for configuration change management, and this would be applied to all Low Impact, Medium Impact, and High Impact systems.

41. Table R23 provide direction concerning what impact level of BES Cyber Systems to which Requirement R23 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree
- Disagree

Comments: See comments under question 40.

**Information Protection and Media Sanitization (R24 – R25)**

42. The definition of sensitive information was derived from the previous version of the CIP standards to minimize disruption to entity information protection programs that are already in place. Do you agree with the proposed definition? Please explain and provide any suggestions for modification.

- Agree
- Disagree

Comments:

43. Do you agree with the proposed definition of Media? Please explain and provide any suggestions for modification.

- Agree
- Disagree

Comments:

44. Requirements R24 and R25 of draft CIP-011-1 concern procedures for information protection and media sanitization. Do you agree with the list of criteria that are included in each Requirements Table for R24 and R25? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

- Agree
- Disagree

45. Tables R24 and R25 provide direction concerning what impact level of BES Cyber Systems to which Requirements R24 and R25 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree
- Disagree

Comments:

**BES Cyber System Maintenance (R26)**

46. The BES Cyber System Maintenance requirement is intended to cover the instances where it is necessary to directly connect a device to the BES Cyber System temporarily to perform a support function, provide appropriate controls on the maintenance device

to protect the BES Cyber System. Do you agree with the definition of maintenance as provided?

- Agree  
 Disagree

Comments:

47. Requirement R26 of draft CIP-011-1 concerns procedures for BES Cyber System maintenance. Do you agree with the list of criteria that are included in Requirements Table R26? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the table? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments:

48. Table R26 provides direction concerning what impact level of BES Cyber Systems to which Requirement R26 applies. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments:

### **Cyber Security Incident Response (R27 – R29)**

49. Requirements R27 to R29 of draft CIP-011-1 concern procedures for Cyber Security Incident response. Do you agree with the list of criteria that are included in each Requirements Table for Requirements R27 to R29? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

- Agree  
 Disagree

Comments:

50. Tables R27 to R29 provide direction concerning what impact level of BES Cyber Systems to which Requirements R27 to R29 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

- Agree  
 Disagree

Comments:

### **BES Cyber System Recovery (R30 – R32)**

51. Requirements R30 to R32 of draft CIP-011-1 concern procedures for BES Cyber System Recovery. Do you agree with the list of criteria that are included in each Requirements

Table for Requirements R30 to R32? Please explain and provide any suggestions for modification. Are there any additional criteria that you believe should be included in the tables? Please explain and provide any suggestions for modification.

Agree

Disagree

Comments:

52. Tables R30 to R32 provide direction concerning what impact level of BES Cyber Systems to which Requirements R30 to R32 apply. Do you agree with the impact levels as indicated? If not, what specific changes would you suggest?

Agree

Disagree

Comments: Item 31.3 could potentially require a large amount of test equipment, when you consider what it would take to develop representative environments for numerous disparate generating facilities and substations. We believe this item should only apply to Control Centers, with testing of the recovery plan (as specified under items 31.1 and 31.2) sufficient at generating facilities and substations.

### General Questions

53. Which requirements in draft CIP-011-1 should allow for TFE submissions? Note that not all requirements will be considered as being applicable for TFE submissions. The drafting team has attempted to minimize the need for TFEs by modifying the language to allow for flexibility in meeting the requirements. Please provide suggestions on how the language of the standard may be modified to eliminate the need for TFEs. If TFEs are still needed, please provide specific examples to justify the inclusion of a requirement as being TFE eligible.

Comments: See comments under questions 17, 34, 35, and 37.

54. Do you have any other comments to improve this version of draft standard CIP-011-1?

We believe all of the requirements that specify something to be completed within X hours would be better suited to the following language: "As soon as practical, but not to exceed x business days from the date reported". This would maintain the spirit of the requirement, while also allowing for more practical time frames.

With so many auditable elements included within the requirements, we believe the VSL's cannot be written with the current zero-defect mentality. We feel a practical approach is required, where minor issues are allowed to be addressed without representing immediate non-compliance and associated investigations and settlement proceedings, but instead are identified and scheduled for corrective action.

We understand the burden on the drafting team to meet FERC's deadlines, but we would propose that all outstanding FERC directives be addressed as part of the current process, as opposed to leaving some items for a later date.