

**Consideration of Comments on Initial Ballot — Urgent Action Revisions to CIP-005-3 (Project 2010-15)**  
**Date of Initial Ballot: September 17, 2010 – September 27, 2010**

**Summary Consideration:** The initial draft of a set of proposed revisions to CIP-005-3 was posted as an Urgent Action under the Reliability Standards Development Procedure – Version 7. Under that process, a proposed standard is posted for a 30-day pre-ballot review, followed by an initial ballot with no formal comment period. While the initial ballot for the proposed revisions to CIP-005-3 achieved a quorum, with 96.46 % of the ballot pool returning a ballot, the weighted segment approval was 21.77%. The drafting team has withdrawn its Urgent Action SAR and proposed a new SAR to address the same issue using the Expedited Process included in the recently approved Standard Processes Manual.

A summary of stakeholder concerns identified with ballot comments and the drafting team’s consideration of those comments has been provided below.

**Definitions:**

“Remote access”

- A definition for “remote access” has been included in the language for the requirement. The definition is “Remote access for the purpose of this standard is user interactive access by a person, used for support and maintenance, which originates from a Cyber Asset not located within any of the Responsible Entity’s Electronic Security Perimeters.”

“Maintenance and support”

- A definition for “maintenance” has been included in the language of the requirements. The definition is “Maintenance for the purpose of this standard includes the activities associated with the support, testing and upkeep of the Cyber Asset within the ESP. Examples of maintenance activities for Cyber Assets within the ESP include configuration changes, power system model maintenance, and application of software patches.”

“Multi-factor authentication”

- Contrary to comments, the drafting team felt that the term “multi-factor” is a defined industry term, which is explained in the associated guidance document, and therefore, no definition is included in the language of the requirements.

“Intermediate device”

- The term “intermediate device” is now followed in the requirements language by the term “proxy server”, which is an industry defined term. No definition of “intermediate device” is included in the language of the requirement, but the concept is discussed in the associated guidance document.

**Consistent use of terms:**

- Numerous comments were received concerning the inconsistent use of terms, specifically the use of “host”, “node”, “remote node” or “device” when referring to Cyber Assets. The requirement has been rewritten to consistently refer to “Cyber Assets”.

#### **Encryption:**

- Numerous comments were received concerning the requirement to provide encrypted communications all the way to the Cyber Assets inside the ESP. This was an oversight on the part of the drafting team, and has been removed. Encryption is now only required when remote access is being initiated from “public networks” (and a definition of “public network” has been included as “public networks are defined for purposes of this standard as a network outside the control of the Responsible Entity”). Since there is no longer a requirement for encryption within the ESP, or within company controlled networks, the drafting team feels that the requirement is justified and not onerous. To the comments about encryption describing a “how” rather than a “what”, the drafting team believes that the requirement for data protection applies to all of the three fundamental tenants of security (integrity, availability and confidentiality), and as such provides a more easily understood requirement. Note that specific encryption technology is not specified in the standard.

#### **Relationship with CAN-0005**

- Commenter’s raised the issue of conflicts between the proposed revisions in this standard and CAN-0005. There are neither conflicts nor contradictions; rather, the two efforts complement each other. CAN-0005 specifically refers to laptops performing system operator functions, while the revisions to CIP-005 specifically refer to remote access for the purpose of support and maintenance.

#### **Multi-factor authentication**

- In addition to the issue raised about a definition for multi-factor authentication, commenters were concerned that the Cyber Assets within the ESP could not support multi-factor authentication. The drafting team has re-written the requirements to address this issue by requiring multi-factor authentication to be performed prior to access to the Cyber Assets within the ESP. The multi-factor authentication can be performed at an interface point to a public network (e.g., when access is initiated from the Internet), or during the authentication process to gain access to a corporate network.

#### **Technical Feasibility Exceptions**

- Commenters requested a provision to request Technical Feasibility Exceptions to the new requirement. The drafting team has re-written the requirements, and believes that the modified requirements can readily and economically be met without requiring technical feasibility exceptions, except in the case of logging remote accesses. Example configurations are provided in the guidance document for a variety of implementations.

#### **Logging duration of access**

- The requirement has been modified to require logging of the login time and logout or disconnect time, instead of login time and duration, and a technical feasibility exception has been allowed.

#### **Dial-up:**

- Commenters requested whether the new requirement applies to dial-up connections. Using the definition of “remote access” in the revised requirements language, yes, dial-up qualifies as remote access (i.e., it is being initiated from a Cyber Asset not located within an entity’s ESP). If the dial-up access is being used for support and maintenance purposes, then the new requirement applies.

#### **Comments concerning Requirement R4 (or other requirements or sections of the standard):**

- This standards action has only proposed changes related to the new Requirement R6, which replaces Requirement 2.4. The scope of the action is limited to modifications pertaining to remote access, not to vulnerability assessments or other sections of the standard. The commenter is urged to provide comments on the vulnerability assessment requirements, when appropriate, to the Cyber Security Order 706 Standard Drafting Team (Project 2008-06).

#### **Comments concerning formatting**

- Commenters questioned why the standard was not converted to the “new” format without sub-requirements. The working group limited itself to technical changes associated with remote access, and adapted all of its additions to the existing style of the standard. Future standards activity by the Cyber Security Order 706 Standards Drafting Team will make the appropriate formatting changes to conform the standard to the most current style.

#### **Implementation Plan:**

- The working group has revised the implementation plan and effective date language. The “effective date” of CIP-005-4 uses the same language as other “Version 4” standards in development, and expected to be file concurrently with the revisions to CIP-005-4, of “Effective Date: The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required).” In light of the need to purchase and install additional equipment to meet the new requirement, an additional six months is proposed before entities are expected to be compliant with the new requirement, making the implementation of the new requirement a minimum of 12 months following regulatory approval of the standard.

#### **Re-numbering of Requirement R2.4**

- Commenters expressed concern that the deleted requirement caused subsequent requirement to be re-numbered, leading to unnecessary compliance documentation updates. When a requirement is deleted the numbering of the requirements is automatically adjusted. This is a standard practice for all NERC standards.

#### **Prescriptive requirements (jump host)**

- Commenters indicated that the requirement for an “intermediate device” was prescriptive, describing how the requirement must be implemented, rather than describing what must be performed. The Drafting Team believes that there are many different technologies that can

be implemented as the required intermediate device, and a more generic description of the requirement would be either a) more confusing to the reader, or b) be able to be interpreted as a weak security implementation. The requirements language has been modified to refer to “an intermediate device or proxy system”, with further elaboration provided in the examples provided in the guidance document.

If you feel that the drafting team overlooked your comments, please let us know immediately. Our goal is to give every comment serious consideration in this process. If you feel there has been an error or omission, you can contact the Vice President and Director of Standards, Herb Schrayshuen, at 609-452-8060 or at herb.schrayshuen@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.<sup>1</sup>

Voter	Entity	Segment	Vote	Comment
Rodney Phillips	Allegheny Power	1	Negative	<p>Allegheny Power is not voting in favor of this standard due the following significant deficiencies and issues:</p> <ol style="list-style-type: none"> <li>1) the currently written draft is ambiguous in part because the terms External and Remote are not defined;</li> <li>2) where the standard implies differences based on the originating location of the access then additional terms “Private Network” and “Public Network or Uncontrolled Private Network” should be used where appropriate as clarification;</li> <li>3) several requirements specify a single technical solution, such as traffic encryption, rather than allowing for alternate solutions that achieve the same goal;</li> <li>4) this standard should not duplicate requirements from other standards, but rather reference those requirements.</li> </ol>
Kirit S. Shah	Ameren Services	1	Negative	<p>In all of R6 the term “remote access” should be changed to “interactive remote access”. R6.4. should be reworded to “Implement intermediate controls such that the external system used for interactive remote access does not communicate directly with Cyber Assets critical to the operations of the BES. “ Multifactor authentication needs to be defined. Our suggestion is Multifactor authentication is Authentication from more than one discrete source/system</p>

<sup>1</sup> The appeals process is in the Reliability Standards Development Procedure: [http://www.nerc.com/files/RSDP\\_V6\\_1\\_12Mar07.pdf](http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf).

Voter	Entity	Segment	Vote	Comment
Paul B. Johnson	American Electric Power	1	Negative	<p>AEP recommends a longer Implementation Plan. Getting this implemented in a complex, multi-ESP environment while preserving reliability is a significant effort. Purchasing and implementing hardware quickly, while following procedures for change management is simply not possible in a six to nine month period and AEP feels that 12 to 18 months might be more appropriate.</p> <p>AEP is requesting clarity on what constitutes "remote access"? There are at least three scenarios for where the traffic originates: 1) internet, 2) corporate network, 3) another ESP. Which one(s) constitute remote access? AEP would assert that at least #3 is not "remote access" and quite possibly not #2 as well. As such, the drafting team should consider explicitly excluding hosts within a separate ESP from the remote access standard.   Further, machine-to-machine ("non-interactive") access may need to be excluded from remote access, even if it involves a machine outside of the ESP.</p> <p>In addition, the change to CIP-005 appears to introduce unnecessary overlap with other standards and requirements.</p> <p>Below are some specific comments in the requirements of CIP-005.</p> <p>R6.1 - This text doesn't belong in CIP-005 as it is a user management issue. This requirement belongs, more properly, in CIP-004, R4. It appears to overlap, and perhaps conflict with CIP-004, R4. If you're compliant with CIP-004, R4 presumably you should be able to demonstrate compliance with CIP-005,</p> <p>R6.1. Demonstrating compliance twice seems unnecessary and cumbersome.</p> <p>R6.2 - There are significant technical issues around duration of access, and yet there is little reliability value. Proving you have the duration of access for each user access appears to be enormously time consuming and resource intensive. If there is no reliability value to tracking duration of access (and it appears there is not), we suggest that it be removed from the requirement. If it remains in the requirement, Responsible Entities will</p>

Voter	Entity	Segment	Vote	Comment
				<p>have to demonstrate compliance - and RE auditors will have to measure it.</p> <p>R6.3 - When and where exactly would encryption be required? Which remote access scenarios would require encryption? Is encryption to the intermediate device in R6.4 sufficient?</p> <p>What is the purpose of the "encryption"? Is it to preserve the confidentiality of the data? If so, why? Is it to provide data integrity? AEP would recommend striking the requirement for encryption. It's very difficult to demonstrate compliance, and appears to add little reliability value.</p> <p>R6.4 - At a minimum, recommend broadening the definition of intermediate device to include the Electronic Security Perimeter Access Point itself. There are many different ways to implement this security control, and as written, this requirement seems to expect a very specific technical solution. Further, for multiple ESPs, a single intermediate device should be sufficient - assuming it's within an equivalent ESP. As discussed above, ESP-to-ESP traffic should be explicitly excluded from "remote access."</p>
Jason Shaver	American Transmission Company, LLC	1	Negative	<p>ATC is balloting negative for the following reason. Requirement 6.3.1 states that an entity has to "provide encrypted communication between the remote node and the host inside of the Electric Security Perimeter". We are concerned that if this practice is implemented an entities intrusion detection system would be unable to identify an intrusion. We recommend that this requirement be changed to say "provide encrypted communication between the remote node and the intermediate device that resides outside of the ESP".</p>
Robert D Smith	Arizona Public Service Co.	1	Affirmative	<p>AZPS Feedback to NERC SAR 2010-15</p> <p>Feedback</p> <p>AZPS generally agrees with the proposed enhancements to CIP-005-3 that resolve potential ambiguities with previous versions of this Standard. AZPS also suggests the following clarifications to further avoid unnecessary Requirement numbers and reduce potential sources of confusion.</p> <p>Suggested Modifications</p>

Voter	Entity	Segment	Vote	Comment
				<p>AZPS suggests that R2.4 be removed to reduce unnecessary separation of requirement numbers, as follows:</p> <p>R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) <u>which shall, at least, identify and describe:</u></p> <p><del>R2.4. The required documentation shall, at least, identify and describe:</del></p> <ul style="list-style-type: none"> <li><del>R2.43.1. The processes for access request and authorization.</del></li> <li><del>R2.43.2. The authentication methods.</del></li> <li><del>R2.43.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.</del></li> <li><del>R2.43.4. The controls used to secure dial-up accessible connections.</del></li> </ul> <p>AZPS further suggests that R6.3 and R6.4 may be confusing, as the requirements to ensure encrypted communications between the remote node and the host inside the ESP seem to conflict with the requirement to implement an intermediate communication device or system. The addition of R6.3.2 may also be confusing, as it seems unnecessary to require that these protocols support R6.1 since implementing protocols that are not compliant with R6.1 should result in a state of non-compliance. It also seems possible that R6.3.1 may result in an encrypted communication stream that reduces the ability to monitor activity at the perimeter (e.g. monitoring activity within the session, which may require access to unencrypted data) and may prove problematic as some Cyber Assets within an ESP may not support encrypted remote access protocols (e.g. RDP).</p> <p>AZPS also suggests merging R6.3 and R6.4, removing the potential conflicts and still allowing for enhanced monitoring capabilities. Suggested modifications are as follows:</p> <p><del>R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that:</del></p> <ul style="list-style-type: none"> <li><del>R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter.</del></li> <li><del>R6.3.2. Support authentication controls sufficient to verify that the</del></li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p><del>individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1.</del></p> <p><del>R6.4. Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset</del></p> <p><u>R6.3. Implement an intermediate device or system for remote access at the Electronic Security Perimeter such that:</u></p> <p><u>R6.3.1. The external system used for remote access does not communicate directly with a Cyber Asset.</u></p> <p><u>R6.3.2. Encrypted communications are ensured between the remote node and the intermediate device.</u></p>
Doug Smeall	ATCO Electric	1	Negative	<p>R6.4: There is a lack of clarity as to where the intermediate device will be located - inside or outside the Electronic Security Perimeter. Location of this device within the Electronic Security Perimeter will necessitate the duplication of applications and support information and the administration of those applications and information on this device, and hence create additional work and potentially require additional resources. Also there is no guarantee that applications will run on this intermediate device.</p>

Voter	Entity	Segment	Vote	Comment
John J. Moraski	Baltimore Gas & Electric Company	1	Negative	<p>CIP-005 comments NERC standards are challenged to clearly define the standard's goal without being overly prescriptive in achieving the goal. The revisions proposed in CIP-005-4 do not yet clearly identify what the standard seeks to achieve, but spells out rather detailed requirements. It is unclear that the prescriptive nature of the proposed requirements is warranted. Remote access needs to be more clearly defined to avoid restrictions on communication between Electronic Security Perimeters (ESP). Requiring remote access in between ESPs would reduce effectiveness of existing security controls assuming that remote access between ESPs could be installed. Additionally, system reliability could be affected if remote access between ESPs reduces availability of CCAs.</p> <p>R6.1.3: Since 6.1.2 establishes the record of individuals with authorized remote access and is referenced, the concluding phrase is unnecessary. Proposed edit: R6.1.3 As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls are implemented pursuant to Requirement R6.2.</p> <p>R6.2.2: Please clarify that the trigger of user logging occurs at the ESP level. Proposed edit: R6.2.2 Implement and document one or more electronic or manual processes for monitoring and logging user identification, and the time and duration of remote access through the Electronic Security Perimeter. R6.3: This requirement is repetitive and unnecessary. R3 and R6.1 already cover the requirements in R6.3. R6.4: Please clarify the intent of this requirement. It does not seem feasible to prevent direct communication with a Cyber Asset. Proposed edit: R6.4 Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Critical Cyber Asset.</p>
Gordon Rawlings	BC Transmission Corporation	1	Negative	<p>The proposed revisions should indicate "what" is required rather than "how" to comply. For example, Requirement R6.3.1 requires encryption between the remote host and the host within the Electronic Security Perimeter (ESP). The requirement should require that communications from the remote host to the access point to the ESP or intermediate device should be protected from tampering. Encryption is one method but others should be allowed if they can ensure confidentiality and integrity. The proposed standard may also cause confusion between or be inconsistent with other existing CIP standards. For example, R6.1.1 limits access to</p>

Voter	Entity	Segment	Vote	Comment
				specific entities while CIP-004, R4 requires a list of authorized personnel. Lastly there is no definition of "remote access" in the proposed standard.
Eric Egge	Black Hills Corp	1	Negative	<p>R6:</p> <ul style="list-style-type: none"> <li>• Move to Follow R2</li> <li>• The definition of "Remote Access" isn't clear. It is not defined in the NERC Glossary or anywhere in this standard.</li> </ul> <p>R6.1.2:</p> <ul style="list-style-type: none"> <li>• change to "annually"</li> </ul> <p>R6.2.1:</p> <ul style="list-style-type: none"> <li>• The implementation and maintenance for this requirement regarding vendors would be difficult to implement and manage, as well as creating risk in response time for support. Would suggest alternate wording to multifactor, multilayer, or other strong authentication mechanisms...</li> </ul>
Donald S. Watkins	Bonneville Power Administration	1	Negative	<p>Unanimous consensus of reviewers is a 'no' vote to these changes. All felt that the proposed changes do not contribute substantively to the current version. The previous version was sufficient. Reviewers also objected to being directed on "how" to comply as opposed to "what" to be complied with. Reviewers also agreed that this draft needs a better definition of "Remote Access." For example, is it access from location external to ESP? Or, is it access from outside controlled networks but within the Responsible Entity's system? Or, is it access from a location that external to the Responsible Entity's systems altogether?</p> <p>Other than the new definition of "Annual" nothing was found to be agreeable within the proposed changes.</p> <p>Comments and Recommendations are listed below.</p> <p>The existing CIP-005-3 R2.4 makes is clear that strong procedural and technical controls must be implemented to ensure "authenticity" of the access party. In some cases, that could mean encryption. It would be helpful to have a Security Guideline for CIP-005 that gave examples of strong technical and procedural controls.</p>

Voter	Entity	Segment	Vote	Comment
				<p>A definition of "remote access" needs to be established.</p> <p>R6 states "...implement the following controls before granting access." It would be best to implement technical and procedural controls once to support remote access and handle granting access authorizations separately.</p> <p>R6 may conflict with the current CIP-005 R3.1 which includes the verbiage "where technically feasible." Since TFE's are not allowed in the future, shouldn't the "where technically feasible" language be deleted? The new R6 should apply to dial-up.</p> <p>R6.1 is redundant with R2.4.1 (currently R2.5.1). We understand that CIP-005-3 R2.4 and R2.5 pertain only to external user interactive access (remote user access) thru the ESP for access to one or more Cyber Assets. Access to ESP ACMs (access control and monitoring) cyber assets is address by CIP-005 R1.5. If a new CIP-005 R6 requirement to address remote access is added, then the current CIP-005-3 R2.4 and R2.5 should be deleted and included in the new R6.</p> <p>R6.1.2 and R6.1.3 are redundant and conflict with the current CIP-005 R2.5.3.</p> <p>R6.2.2 and R6.2.3 are somewhat redundant with the current CIP-005 RCIP-005 R3.2.</p> <p>R6.4.The intermediate device or system for remote access should not be an external system.</p> <p>A suggested rewording</p> <p>R6. Remote Access Controls - To prevent unauthorized access to its Cyber Assets, where interactive access into the Electronic Security Perimeter is to be enabled, prior to granting such access the Responsible entity shall:</p> <p style="padding-left: 40px;">R6.1. Implement and document procedural and technical controls to ensure that such access is controlled and limited to authorized personnel.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.2. Restrict remote access to Electronic Security Perimeter access points to methods which support authentication controls sufficient to verify the identify and authenticity of individuals remotely accessing Cyber Assets within the Electronic Security Perimeter.</p> <p>R6.3. Provide logging of all successful and failed access attempts.</p>
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	The new requirement R6.4 should provide for a technically feasible exception.
Paul Rocha	CenterPoint Energy	1	Negative	<p>The proposed changes to CIP-005-3 cannot be implemented as written; therefore, CenterPoint Energy is submitting a NEGATIVE vote. In addition to the many technical issues identified below, CenterPoint Energy is concerned the proposed requirements could negatively impact an entity's ability to maintain Critical Cyber Assets and therefore have the unintended consequence of reducing reliability of the BES.</p> <p>An intermediate device or system (R6.4, i.e. proxy) used for remote access to a Cyber Asset within the ESP makes R6.2.1 and R6.3.1 unnecessary. Furthermore, if the intermediate device or system (i.e. proxy) is located external to the ESP, the intermediate device or system (i.e. proxy) will be an external system that cannot communicate directly with a Cyber Asset within the ESP according to R6.4.</p> <p>CenterPoint Energy is concerned some legacy systems may not be able to support R6.4 and therefore strongly recommends that R6.4 be modified as follows:</p> <p>R6.4 Where technically feasible, implement an intermediate device or system in conjunction with R6.1, R6.2 and R6.3 such that the external system used for remote access does not communicate via IP directly with a Cyber Asset within the ESP.</p> <p>CenterPoint Energy strongly recommends the following updates be made to the draft:</p> <ul style="list-style-type: none"> <li>Clarify the intent of R6 (to be applied to interactive remote access</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>only).</p> <ul style="list-style-type: none"> <li>• Maintain clarity with the thought of interactive or programmatic remote access to Cyber Assets within the ESP versus interactive or programmatic remote access to the access control devices protecting the Cyber Assets within the ESP throughout the standard.</li> <li>• Modify the statement in R6, "If a Responsible Entity wants to grant ..... " to "If a Responsible Entity allows remote access.....". Replace "granting" with "allowing".</li> <li>• Add "interactive" in front of "remote access" in R6.2 and R6.2.1.</li> <li>• Add "Cyber Assets" before "to (within) the Electronic Security Perimeter" in R6.2.</li> <li>• R6.3 Restrict the IP communications allowed to pass through an ESP access point to:</li> <li>• M6 references "...device controls as specified in Requirement R6". "Device controls" are not referenced in R6. CNP recommends deleting the word "device" in M6.</li> <li>• In the Version History table, "Critical Assets" should be changed to "Critical Cyber Assets".</li> <li>• Technical Feasibility Exceptions (TFEs) should be included for requirements R6.2, R6.3 and R6.4 for legacy system limitations and third-party dependencies.</li> </ul>
Chang G Choi	City of Tacoma, Department of Public Utilities,	1	Negative	Tacoma Power supports the development of this Standard and is of the opinion that the draft implementation guidelines provided by NERC offers best security practices and sound architectural solutions that would

Voter	Entity	Segment	Vote	Comment
	Light Division, dba Tacoma Power			<p>mitigate the security issues the revised CIP-005-4 Standard seeks to address.</p> <p>While we have read and appreciate the technical concerns raised by other entities, Tacoma Power supports APPA's position that the draft implementation guidelines provided by NERC offer a solution intended to protect BES critical cyber assets from a real vulnerability of Virtual Private Networks ("VPNs") that is known by federal agencies to have in fact been exploited.</p> <p>Unfortunately, Tacoma Power, while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a "Yes" vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>Tacoma Power suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. Tacoma Power feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define "remote access".</li> <li>2. 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 Seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>3. 6.1.2 requires that the access lists be reviewed “yearly” and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</p> <p>4. 6.1.3 Also seems to be redundant with CIP-004-3 R4.</p> <p>Thank you for your consideration in this matter.</p>
Danny McDaniel	Cleco Power LLC	1	Affirmative	None
Christopher L de Graffenried	Consolidated Edison Co. of New York	1	Negative	<p><b><u>CIP-005-4 Comments</u></b> - Consolidated Edison supports NPCC’s comments.</p> <ul style="list-style-type: none"> <li>• An implementation plan has not been posted.</li> <li>• The SAR is too broad in its scope. The SAR should be more specific on the type of Remote Access covered.</li> <li>• Why does the SAR’s Brief Description use “devices” instead of the defined term Cyber Asset? “A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)”.</li> <li>• The updates to CIP-005 do not respond to the SAR’s intent of end point protection. The updates only address access across the Electronic Security Perimeter (ESP)</li> <li>• The current R6 repeats many requirements already specified in R2. The contents of R6 should be moved as a sub-requirement of R2, R2.3 being the corresponding stricken requirement. As posted, some sub-requirements of R6 result in a double jeopardy.</li> <li>• The term “remote access” used in R6 needs clarification. Instead of “remote access” suggest using “remote interactive user access to Cyber Assets in the ESP from outside of the ESP”</li> <li>• The language for R6 requires clarification to more accurately reflect the intended scope, specifically as follows: <ul style="list-style-type: none"> <li>○ Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and</li> </ul> </li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</p> <ul style="list-style-type: none"> <li>○ CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>○ It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer.</li> </ul> <ul style="list-style-type: none"> <li>• Requirement R6.1 should be removed: it duplicates CIP-004 Requirements, resulting in double jeopardy.</li> <li>• Requirement R6.2 should be removed: it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</li> <li>• There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural (i.e. a multifactor authentication scheme can be implemented by any mix of technical and procedural controls). By putting this under technical requirements this requirement implies that only technical solutions are acceptable.</li> <li>• Requirement R6.3 duplicates the ports and services requirements in CIP-005 R4.2: it should be removed.</li> <li>• Requiring encryption across the ESP in requirement R6.3.1 to the end-device inside the ESP is against the best practice implemented by many entities of decrypting at or immediately prior to the access point. Encrypting beyond the access point removes the visibility required for content inspection as risk mitigation control.</li> <li>• Requirement R6.4 prescribes a specific mitigation control, telling how to implement. The Requirement should be redrafted to specify the control objective and allow entities to implement the specific controls required to achieve the control objective.</li> </ul>
John K Loftis	Dominion	1	Negative	Dominion believes properly authorized personnel must be allowed to

Voter	Entity	Segment	Vote	Comment
	Virginia Power			<p>provide remote operational and maintenance support for cyber assets within an Electronic Security Perimeter to maintain reliable operation of the Bulk Electric System. The application of remote access security measures should be carefully applied to avoid inadvertent, adverse reliability impacts. Several specific issues with proposed CIP-005-4 R6 changes must be addressed before the new requirement can be properly interpreted and consistently implemented throughout the industry.</p> <p>R6.1 – This requirement duplicates access control requirements addressed in CIP-005 R2 and CIP-004 R4. Dominion suggests moving requirement R6.1.1 to requirement R2 as a sub-requirement to R2.1. Requirement R6.1.2 repeats and may even contradict access authorization requirements in CIP-004 R4 regarding the review and validation of personnel with authorized cyber access to Critical Cyber Assets (e.g., quarterly access reviews vs 15 months for ESP access). Dominion suggests referring to requirement CIP-004 R4 or CIP-005 R2 (which refers to CIP-004 R4) instead of specifying separate review requirements in R6.1.2 and R6.1.3. If the requirement to validate who has remote access to an ESP once a calendar year is kept, please define a calendar year and clarify how a review is conducted ‘at least once each calendar year, with no more than 15 months between reviews’.</p> <p>R6.2.1 – The deletion of existing requirement R2.3 removes the reference to ‘external interactive access into the Electronic Security Perimeter’. However, the reference to multifactor authentication in this requirement suggests the term ‘remote access’ refers to interactive user access. Do the remote access requirements apply to remote devices that poll devices inside an ESP or data connections between multiple ESPs? The term ‘remote access’ should be more clearly defined.</p> <p>Based on FERC Order 706 paragraph 511, the reference to multifactor authentication is too prescriptive. That Order cited two-factor authentication and digital certificates as <i>examples</i> of strong authentication but did not specify that they were the only methods allowed.</p> <p>R6.2.2 – Dominion questions the feasibility of monitoring and logging the <i>duration</i> of remote access sessions. If this requirement remains, a Technical Feasibility Exception (TFE) should be allowed. Monitoring and logging requirements are already addressed in requirements R3 and R5 of CIP-005 and should be removed from R6.2.2 and R6.2.3.</p> <p>R6.3 – Serial connections via dial-up modems cannot support protocol/port</p>

Voter	Entity	Segment	Vote	Comment
				<p>restrictions or encrypted communications. Dial-up access is addressed in CIP-005 R2. Does CIP-005 R6 apply to dial-up access?</p> <p>R6.3.1 – According to the Purpose statement in the Introduction section of proposed standard CIP-005-4, the standard focuses on the identification and protection of the Electronic Security Perimeter (ESP) and perimeter access points. However, requirement R6.3.1 specifies encryption between a remote node and devices inside the ESP instead of between a remote node and an access point. This practice would prohibit adequate inspection at the access point to insure access has been authorized. The requirement only recognizes end-to-end encryption and does not permit the use of network level encryption.</p> <p>Encryption from a remote access point to a host inside the ESP may not be technically feasible for all device types and precludes intrusion inspection of the traffic through the access point. If this requirement stands a Technical Feasibility Exception (TFE) should be allowed.</p> <p>R6.4 - The requirement to 'implement an intermediate device or system' to communicate remotely with a cyber asset within an ESP appears to contradict requirement R6.3.1, which suggests that the remote node must communicate directly with the host using encrypted communications. (In addition, isn't the intermediate device itself a remote node?) Please define 'intermediate device or system'.</p> <p>In general, Dominion supports the following measures for remotely accessing cyber assets within an ESP:</p> <ul style="list-style-type: none"> <li>• Multifactor authentication for interactive access.</li> <li>• Introduction of an intermediate device or system so interactive access from an external device does not communicate directly with a cyber asset within an ESP.</li> <li>• Use of encryption from a remote device to an ESP access point</li> </ul> <p>Requiring that 1) anyone granted remote access to an ESP has access to protected devices inside the ESP, and 2) removal of access to all devices inside an ESP requires removal of remote access to the ESP.</p>

Voter	Entity	Segment	Vote	Comment
Ralph Frederick Meyer	Empire District Electric Co.	1	Negative	We appreciate the effort by the drafting team, however we have cast a negative vote for the following reasons: R6.2.1 states that multifactor authentication would be used for establishing remote access to Cyber Assets. It is unclear if this this mean that the VPN authentication counts as one and the asset's login counts as another. This should be clearer to define if multiple factors need to occur prior to contacting the asset from a VPN session for example? R6.2.2 states that the duration of the remote access needs to be documented. The level of documentation required for compliance should be further explained. ?R6.4 This statement needs to be clearer for situations were a connection directly to the asset is using a VPN connection. This would seem to indicate that the vendor must connect to a intermediate system which would then connect to the asset. Does this require another system to be configured and placed outside EMS perimeter to be used for connecting to EMS Cyber Assets?? This is rather confusing because if it were inside then it would be a Cyber Asset too?? Clarity is needed with the entire 6.4
Robert Martinko	FirstEnergy Energy Delivery	1	Negative	FE believes clarifications are required for the proposed standard and therefore casts a Negative vote with the following suggestions: R6.2.3 - We recommend the deletion of R6.2.3 as data retention is already covered in R5.3. Also, we do not agree that retention of information for investigations should be mandated in a reliability requirement. The retention of information for an investigation is applicable to any standard requirements as specified by the Regional Entity conducting the investigation. This is further reinforced in section 1.3.1 of the Data Retention section of the standard. R6.3.1 - We suggest rewording the requirement to "Provide encrypted communications between the remote node and the Electronic Security Perimeter access control device." We suggest this change because there is no encryption of data traffic "inside" the ESP. R6.3.2 - Requirements R6.3.2 and R6.2.1 appear duplicative. Therefore we suggest deleting R6.3.2 and rewording R6.2.1 as follows: "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter that are sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1."
Harold Taylor, II	Georgia Transmission Corporation	1	Negative	GTC appreciates the working group addressing this vulnerability through the urgent action process and hopes that it uses this initial ballot period to address the concerns that we have listed below. - The draft standard for

Voter	Entity	Segment	Vote	Comment
				<p>CIP-005-4 lays out requirements that are technically impossible (encryption to the host, R6.3.1) for GTC in some scenarios, but does not allow for a TFE. - R6.3.1 is not consistent with best practices. Best practices dictate that all encrypted tunnels be terminated outside of an ESP or at the access point to the ESP such that an intrusion detection system (IDS) can inspect the traffic at the ingress point. - Remote access is not defined. This standard could possibly extend to machine-to-machine interactions which would make this standard impossible to implement. - Remote access is limited by R6.1.1 for only "technical support" purposes. The purpose of accessing devices remotely should not be limited by the standard. - The standard does not sufficiently allow for vendors to access systems remotely for the purpose of support. At times, vendor access to systems is critical and you are unable to determine who that individual may be prior to calling a vendor's support line. - Multifactor authentication is undefined. This term needs more clarity in order for entities to reasonably understand how to meet compliance. - There is a lack of clarity on R6.1.1 which indicates limiting access to personnel who have "authorized electronic access." CIP-004 R4 requires that a list be kept for personnel who have "authorized cyber access." Are these different lists? What exactly is the difference or are they equivalent? Why were different words chosen? - R6.4 requires that access be provided through an intermediate device, but does not provide clarity on how this intermediate device must be managed. Does the intermediate device or system required in R6.4 become a Critical Cyber Asset? Must this system reside inside the ESP with the CCA it is providing access to, does it have to reside in its own ESP, or is it not required to reside in an ESP? Does this system fall under the requirements of CIP-005 R1.5?</p>
Robert Solomon	Hoosier Energy Rural Electric Cooperative, Inc.	1	Negative	<p>The language needs to be more specific on defining "remote access". The language being deleted, CIP-005-3 R2.3 specifically addresses Interactive access to the ESP. The new requirement, CIP-005 R6.x, does not, it only refers to "remote access". The language is too loose regarding what "remote access" is and what includes.</p>

Voter	Entity	Segment	Vote	Comment
Ajay Garg	Hydro One Networks, Inc.	1	Negative	<p>Hydro One is casting a negative vote for the following reasons:</p> <ol style="list-style-type: none"> <li>1. There is no implementation plan accompanying the proposed standard.</li> <li>2. The industry did not have an opportunity to request clarification on what "remote access" means to provide a more accurate scope for the SAR. Questions such as: What type of remote access? What is this SAR trying protect? should be answered.</li> <li>3. Why the SAR's Brief Description does uses the term "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)." We believe that Cyber Assets can even include smart-phones like Blackberry.</li> <li>4. The updates to CIP-005 do not respond the SAR's intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP).</li> <li>5. We believe that the new R6 should replace the stricken R2.3 since, as written, it creates the possibility of violating two Requirements by the same event (double-jeopardy).</li> <li>6. We do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security</li> </ol> <p>In addition, we recommend the following:</p> <ol style="list-style-type: none"> <li>(a) Clarify "remote access" in R6. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP"</li> <li>(b) The language for R6 must be clarified to more accurately reflect the intended scope, specifically to the following: <ul style="list-style-type: none"> <li>• Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>• The CAN-005 document appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> </ul> </li> </ol>

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> <li>It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access.</li> </ul> <p>(c) The language in the version history log needs to be clearer.</p> <p>(d) Remove R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy.</p> <p>(e) Remove R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</p> <p>(f) There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural; putting this under technical requirements implies that only technical solutions are acceptable.</p> <p>(g) Remove R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2.</p> <p>Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>
Bernard Pelletier	Hydro-Quebec TransEnergie	1	Negative	There is no definition of "Remote access". Depending on the definition, the impact of this change could be very significant. Multifactor authentication should be used when it's coming from an external (non-controlled) network into a controlled network. Clarification is needed for `communicate directly with a cyber asset` (proxy, routed vs. Non-routed, "natted" via ESP entry point, etc...). Hydro Quebec will changed the vote to YES when corrections are made.
Ronald D. Schellberg	Idaho Power Company	1	Negative	The proposed changes do not contribute substantively to the current version of CIP-005. The proposed standard also indicated that the proposed revisions should indicate "what" is required rather than "how" to comply. For example, Requirement R6.3.1 requires encryption between the remote host and the host within the Electronic Security Perimeter (ESP). The requirement should require that communications from the remote host to the access point to the ESP or intermediate device should be protected from tampering. Encryption is one method but others should be allowed if they can ensure confidentiality and integrity. Additionally the proposed standard may cause confusion between or be inconsistent with other

Voter	Entity	Segment	Vote	Comment
				existing CIP standards. For example, R6.1.1 limits access to specific entities while CIP-004, R4 requires a list of authorized personnel. Also, there is no definition of "remote access" in the proposed standard.
Michael Holtsclaw	Indianapolis Power & Light Co.	1	Negative	<ol style="list-style-type: none"> <li>1. R6. Add "Critical" before "Cyber Assets..." in last line.</li> <li>2. The proposed language in R6.1.1, "Limit access to only the Responsible Entity's personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter", creates two classes of individuals with access. To maintain continuity to the proposed R6.1.2 and R6.1.3, suggest rewording R6.1.1 to: "Limit access to only the individuals who have authorized electronic access to Critical Cyber Assets within the specific Electronic Security Perimeter. "</li> <li>3. R6.1.2 would seem to be covered adequately in CIP-004-3 R4. Suggest removing R6.1.2.</li> <li>4. The duration requirement proposed in R6.2.2 will be technically difficult to achieve as remote connections can be dropped without the terminating node realizing the connection was disconnected. Suggest removing the duration component of R6.2.2.</li> <li>5. The log retention specification in R6.2.3 appears to be superfluous considering Part D Â§1.3.1. Suggest deleting R6.2.3.</li> <li>6. R6.3 is unclear in that remote access is insufficiently bounded and the intent is difficult to determine. Does the drafting team intend remote access to be any inbound communications to an ESP? What about: - Remote Access" from a cyber asset within one ESP to a cyber asset within a second ESP? - Remote Access" from a node external to the ESP but internal to a corporate LAN? - Remote Access" from a node remotely accessing the ESP via the corporate LAN? Suggest inserting wording/definition at the appropriate location in which remote access is defined as: "User interactive session which originates from a cyber asset not located within the Entity's Electronic Security Perimeter(s)."</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>7. R6.3.1 is unclear on whether or not the encrypted communications must be end to end (from remote node to host inside the Electronic Security Perimeter). The language infers encrypted communications end to end. Suggest rewording to: "Provide encrypted communications between the remote node and the intermediate device specified in R6.4".</p> <p>8. R6.4 is worded in such a way that the location of the intermediate device or system between the remote node and the host within the Electronic Security Perimeter that performs Network Address Translation (NAT) or Port Address Translation (PAT) is unclear. Suggest adding language to R6.4 to associate it with the Access Point. "Implement an intermediate device or system, associated with an Access Point for the Electronic Security Perimeter, such that the external system used for remote access does not communicate directly with a Cyber Asset." The addition of this language in the previous suggestion will ensure that communication outside of the ESP will be encrypted and that the encryption terminates at the ESP boundary.</p>
Michael Moltane	International Transmission Company Holdings Corp	1	Negative	ITC considered the following as the most dominant reasons for our "NO" vote: Requirement R6.2.1- There is not a definition of the term "multifactor" to enable an adequate implementation and compliance method. Requirement R6.3.1- Encryption requirements aren't clear to whether or not the same implies to and/or from devices within ESPs or end points. Requirement R6.4 - Addition of an external system or device will make an inclusion of such Cyber Asset that will redefine the end point of the connections ; and impact the Electronic Security Perimeter for the Critical Asset.
Michael Gammon	Kansas City Power & Light Co.	1	Negative	These proposed changes to CIP-005 are conflicting and add substantial confusion regarding the principles of remote access to Critical Cyber Assets.

Voter	Entity	Segment	Vote	Comment
Stan T. Rzad	Keys Energy Services	1	Negative	The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too proscriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security. R6.3.1 also could be interpreted to be in conflict with R3. If the communication stream between the remote node and endpoint in the ESP is encrypted, there (should be) no feasible way of logging access attempts, as all of the packets (should be) encrypted according to R6.3.1. R6.3.1 also seems to be in conflict with 6.4, requiring an "intermediate device or system" between the remote node and endpoint in the ESP.
Larry E Watt	Lakeland Electric	1	Negative	A guidance document for the current standard and the inclusion of selected terms in the NERC glossary of terms would meet the intent of this Urgent Action SAR. We question the need for this Urgent Action SAR. We believe that this SAR and the proposed changes to CIP005 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511
Martyn Turner	Lower Colorado River Authority	1	Affirmative	LCRA supports the development of this Standard, but is of the opinion that the following items need to be improved: 6. Remote Access should be defined as unsupervised interactive system access by a person from outside the plant, control system or substation facility location. 6.1.2 The 'yearly' review is in conflict of the quarterly reviews required by CIP 004 R4. Recommend omitting the review requirement, since it is covered more stringently in CIP 004. 6.3.1 Should state "Provide encrypted communications between the remote node and the access point to the ESP." This is due to the fact that not all vendors support encrypted protocols. Providing encryption to the access point of the ESP provides sufficient mitigation against this threat.

Voter	Entity	Segment	Vote	Comment
Michelle Rheault	Manitoba Hydro	1	Negative	<p>General Comments:</p> <p>1. Remote Access: It is unclear whether “remote access” refers to “remote interactive access” of a person to the Cyber Asset, or remote machine-to-machine access with the Cyber Asset. Both these types of access are distinct, and have different security solutions. If the intent is to address the person to Cyber Asset access, and the machine-to-machine Cyber Asset access, then they should be addressed separately in the standard.</p> <p>2. Removal of Technically Feasible: Legacy devices may be unable to meet the prescriptive technical requirements of the proposed R6, and therefore the requirements should only apply where technically feasible, and be subject to the Technical Feasibility Exception process.</p> <p>3. Version History: The standard applies to Cyber Assets, not Critical Assets. The reference to “for support staff maintenance” in the Action is not reflected in the accompanying SAR, which makes vague references to remote access. The proposed standard, as written, could be interpreted to apply to remote access for any purpose. R6 - The current wording is too broad. Suggest wording “The Responsible Entity shall implement the following controls before granting remote interactive access to its Electronic Security Perimeters, to prevent unauthorized access to its Cyber Assets within its Electronic Security Perimeters.” R6.1.1 - Vendor personnel who provide technical support for Cyber Assets within the ESP should also be authorized. Suggest wording “... vendor personnel who have authorized electronic access who provide technical support ...”. R6.2.1 - The current wording could be interpreted as requiring multifactor authentication to, and including, the Cyber Asset within the ESP. Not all Cyber Assets within the ESP will support multifactor authentication. Multifactor authentication to the ESP should be sufficient. R6.3 - The actual intent of Requirement 6.3 is unclear. Regarding the statement “Restrict the protocols ... to protocols that: Provide encrypted communications .... ” Is the intent that the protocol provide the encryption? Not all protocols provide encryption, although other technologies can encrypt communications, but not at the protocol level. Is the intent that the protocol support the authentication? Not all protocols support authentication, although other technologies can support authentication. The intent of the requirement should be to require secure</p>

Voter	Entity	Segment	Vote	Comment
				communications, without being overly prescriptive. The terms “remote node” and “host” are not clear, are not defined, and are not used anywhere else in CIP-003 through CIP-009. R6.3.1 - Requirement 6.3.1 specifies that encrypted communications must terminate at a host within the ESP. VPN tunnels that terminate at a firewall provide the same or a better level of security as VPN tunnels that terminate at an internal proxy server, are a mainstream IT architecture and should not be excluded. This architecture also has the advantage of supporting unencrypted traffic within the ESP, which allows the firewall’s anti-malware software and the IDS sensors inside the ESP to analyze the traffic. The current wording excludes this architecture. R6.4 - The wording, the intent, and the security value of Requirement 6.4 is unclear and this requirement should be removed.
Danny Dees	MEAG Power	1	Affirmative	As stated by MEAG Power on 9/14/10 during the Pre-Ballot Window for this proposed new standard, MEAG Power has concerns about the meaning of the current language being proposed in R6.3.1. MEAG Power is voting “yes” under the assumption that the goal of an entity providing “encrypted communications between the remote node and the host inside the Electronic Security Perimeter” could be accomplished by an entity providing encryption between the remote node and an intermediate device - so that any external system(s) used for remote access does not communicate directly with a Cyber Asset within the Electronic Security Perimeter.
Terry Harbour	MidAmerican Energy Co.	1	Negative	<ol style="list-style-type: none"> <li>Proposed R6 replaces R2.4’s reference to “external interactive access” with “remote access.” “External interactive access” should be retained, consistently referenced throughout CIP-005 in all applicable requirements and defined locally in only CIP-005 as follows: “External interactive access is defined as network access using routable protocol initiated by an end user outside the ESP to remotely control or access a console or terminal based session on another network attached device inside the ESP.”</li> <li>Proposed R6 prescribes “how” to comply and “what is required.” For example, encryption is “how” versus “protect communications” would be “what.” Similarly, requiring an intermediate device or system is “how” not “what.” Proposed R6.2.1 requires “multifactor authentication” and replaces existing R2.4 “strong controls.” Strong controls is “what” whereas “multifactor” is “how” and undefined.</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<ol style="list-style-type: none"> <li>3. Proposed R6.3.1. requires encryption to the host inside the ESP. This is not correct. If encryption is required, it should be to “provide encrypted communications between the remote node to the access point and be available for inspection within the ESP.”</li> <li>4. Proposed R6.1.1.-.3 overlap the remaining new CIP-005 R2.4 and requirements in CIP-004 and CIP-007 R5. Proposed R6.2.2 overlaps CIP-007 logging and alerting. Redundancy should be eliminated.</li> <li>5. Proposed R6.1.2. creates a definition for annual unique to this one requirement. This is unacceptable. A universal definition of annual for all CIP should be adopted through the standard SAR process.</li> <li>6. Proposed R6.2.2 requires documenting duration of remote access. This is contradictory to the approaches for logs in CIP-006 and -007. Should proposed R6.2.2 be addressed with existing CIP-005 R3?</li> <li>7. Overall the proposed revisions create additional undefined terms, prescribe “how” not “what” and introduce confusing redundancy/overlap to other existing standards. Existing R2.4 and R2.5 should be enhanced minimally to achieve the desired result.</li> </ol>
Randi Woodward	Minnesota Power, Inc.	1	Negative	<ul style="list-style-type: none"> <li>▪ Minnesota Power believes that the wording in Requirement 6.3.1 should be revised to require encrypted communications from the remote host to the Electronic Security Perimeter, not to the end host. The existing NERC CIP-002 – CIP-009 Standards do not require encrypted traffic within an Electronic Security Perimeter. This change would require specific technology to provide encryption, such as VPN access, to every asset which is currently not feasible. In addition, if the traffic was encrypted to the end host, then Intrusion Detection Systems would not be effective at analyzing the traffic for malware and viruses.</li> <li>▪ Minnesota Power believes that the term “Remote Access” needs to be specifically defined and consistently applied through NERC Standard CIP-005. We believe confusion exists among Registered Entities about what constitutes “Remote Access” For example, is there, or should there, be a difference between remote access “outside a company” versus “outside an Electronic Security Perimeter, but inside a company”? “Remote Access” could be interpreted to mean all host communications from outside to inside an Electronic Security Perimeter and could inadvertently include things like communications between computers or communications between the RTUs and the Cyber Assets</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>within the Electronic Security Perimeter. We believe that "Remote Access" should be replaced with "Interactive Remote Access."</p> <ul style="list-style-type: none"> <li>▪ Minnesota Power recommends the removal of Requirement 6.2.3 as it is redundant with the existing Requirement 5.3. Requirement 5.3 states: "R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3." and is applicable to NERC Standard CIP-005 in its entirety.</li> <li>▪ Minnesota Power suggests rewording Requirement 6.2.2 from "R6.2.2. Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and the time and duration of remote access to Cyber Assets within the Electronic Security Perimeter." to "R6.2.2. Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and the time of remote access to the Electronic Security Perimeter." Tracking the duration of remote access could prove to be complex and time consuming and would not add much benefit. Also, dropping "Cyber Assets" would ensure consistency with the intent of Requirement 6.3.1 as discussed in our comment above.</li> </ul>
Saurabh Saksena	National Grid	1	Negative	<p>The current proposed Standard appears to not be clear in respects to what is required. Without changes to the Urgent Action to address the issues raised in the comments below, National Grid is voting negative on this standard. National Grid is not opposed to revisiting its position once the corrections on intent, removal of duplication and double jeopardy are addressed.</p> <p>Here are few recommendations:</p> <ol style="list-style-type: none"> <li>1. There is no proposed corresponding implementation plan</li> <li>2. The industry did not have an opportunity to request clarification on what "remote access" means to provide a more accurate scope for the SAR. What type of remote access? What is this SAR trying protect?</li> <li>3. Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter),” We believe that Cyber Asset can include smartphones like Blackberry.</p> <ol style="list-style-type: none"> <li>4. The updates to CIP-005 do not respond the SAR’s intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP)</li> <li>5. Recommend that the new R6 should replace the stricken R2.3 since not moving R6 creates the possibility of violating two Requirements or double-jeopardy.</li> <li>6. Recommend clarifying “remote access” in R6.</li> <li>7. Instead of “remote access” suggest using “remote interactive user access to Cyber Assets in the ESP from outside of the ESP”</li> <li>8. Recommend that the language for R6 be clarified to more accurately reflect the intended scope, specifically to the following: <ul style="list-style-type: none"> <li>· Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>· CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>· It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive</li> </ul> </li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>user access.</p> <p>9. The language in the version history log seems to be clearer.</p> <p>10. Recommend removing R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy</p> <p>11. Recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</p> <p>12. There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural, putting this under technical requirements implies that only technical solutions are acceptable.</p> <p>13. Recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2</p> <p>14. Do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security</p> <p>15. Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>
Richard L. Koch	Nebraska Public Power District	1	Negative	<p>R6.2.1 Comments:</p> <ul style="list-style-type: none"> <li>• Does the RSA authentication system equipment need to be on the inside of the ESP and PSP?</li> <li>• Does the system (server/PC) that authenticates the remote user need to be on the inside of the ESP and PSP? For example, could a system (Windows Terminal Server or dedicated PC) on the outside of the ESP and PSP be used as a workstation that validates user authentication via multifactor authentication? The user then launches an application that then allows them to authenticate to a CCA or non-CCA without multifactor authentication but via the ESP controls limit access by IP address and port.</li> </ul> <p>R6.2.2 Comments:</p>

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> <li>Is the duration of the interactive session in relationship to the first system or all subsequent systems as well? For example, I log into Non-CCA Server A. Server A is inside the ESP. It prompts me for my multifactor authentication as it is the initial system I access through the ESP. From Server A I start a remote session to CCA Server B which is not directly accessible through the ESP. Do I only need log the duration of access to Server A or do I also need to record separately the access duration to Server B?</li> </ul> <p>R6.3.1 Comments:</p> <ul style="list-style-type: none"> <li>What levels of encryption are acceptable? DES, 3DES, Blowfish, AES?</li> <li>Can a VPN tunnel be utilized between the remote node and a VPN appliance on the ESP or does the encryption have to be between the first internal host and the external host communicating into the ESP?</li> <li>If VPN tunnels are allowed, split tunnel configurations should be disallowed.</li> </ul> <p>R6.4 Comments:</p> <p>This seems confusing as all devices within an ESP are either Critical Cyber Assets (CCA) or Non-Critical Cyber Assets (Non-CCA). Is this meant to say "Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a <b>Critical</b> Cyber Asset." or is this to mean that communications are required to go through a control/protection device such as a firewall or inline IDS?</p>
Randy MacDonald	New Brunswick Power Transmission Corporation	1	Negative	It appears that R6 requirements (remote access) overlap with those of R2 and R3. Further refinements of R6 requirements and possibly R2&3 are necessary for clarification. Multifactor authentication requires further clarification
David H. Boguslawski	Northeast Utilities	1	Negative	NU concurs that the vulnerabilities that may exist in remote access methods and technologies need to be mitigated to prevent unauthorized remote cyber access to cyber assets within a defined Electronic Security Perimeter. Although NU concurs with the intent of the proposed revision to CIP-005-3 to prevent unauthorized remote cyber access, NU voted to oppose the revised standard as written. The basis for our oppose vote is

Voter	Entity	Segment	Vote	Comment
				that NU believes that areas of opportunities have been identified by industry stakeholders (including but not limited to EEI and NPCC) that should be considered to improve the proposed revision. For example, it is recommended that terms like remote access, interactive access and multifactor authentication be defined. Additionally, care should be taken to ensure duplicative or redundant requirements are not created. Specifically: - Recommend removing R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy - Recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2. - Recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2
Robert Matthey	Ohio Valley Electric Corp.	1	Negative	Concerned that the wording in R6.1 (specifically R6.1.1) could be interpreted that access to the remote access system implies access to the CCAs when in fact the remote access system may be used to access non-CCAs in addition to CCAs but entry into the electronic security perimeter is restricted. R6.1.2 seems to create additional redundant documentation.
Douglas G Peterchuck	Omaha Public Power District	1	Negative	<ul style="list-style-type: none"> <li>• The term 'remote node' needs to be further defined. Is the intermediate device referred to in R6.4 considered a remote node?</li> <li>• Overall, is the intent of R.6 to define 'interactive' remote access? We feel this is the intent, but this is not clear in all of the requirements. Either state that in the verbiage in the main R.6 requirement or clarify throughout the sub requirements. If this is not clarified, than requirements such as R6.3.1 would possibly require encryption for all communications through an ESP whether interactive or application based.</li> <li>• If an intermediate device is required for a remote access in R6.4, this appears to contradict R6.3.1 which requires encryption from the remote node and the host inside.</li> <li>• If the intermediate box is required, then remove the encryption requirement between the intermediate box and the host inside the ESP.</li> <li>• The term 'multifactor authentication' needs to be further defined.</li> </ul>
Michael T. Quinn	Oncor Electric Delivery	1	Negative	The requirement is unclear whether the personnel referenced in R6.1.1(V4) also must comply with the Requirements of CIP-004 "Personnel and Training", or if this new requirement is an exception to CIP-004 for personnel with cyber access to Critical Cyber Assets (CCA). If this is a exception to CIP-004, then it should clearly state this exception. The

Voter	Entity	Segment	Vote	Comment
				requirement does not differentiate between IP and dial-up accessible CCAs. Many dial-up CCAs are not capable of logging time/duration (R6.2.2), serial encryption (R6.3.1), or authentication as required to satisfy R6.3.2. R6.4 is overly burdensome for Electronic Security Perimeters that contain only dial-up accessible CCAs. R6.4 should include this clarification in wording, "does not communicate directly with a Cyber Asset inside the Electronic Security Perimeter."
Brad Chase	Orlando Utilities Commission	1	Negative	R6 is currently very poorly worded and suggest changing the wording to the following to remove ambiguity in using words such as "if" and "wish" and remove the interpretation surrounding the word "remote": Remote Access Controls - The following controls shall be implemented for all access to Cyber Assets across an ESP boundary: Additionally, Requirement 6.3.1 could be in direct contradiction to requirement 6.4. if encryption between a remote node and a host node is interpreted to be a serial chain of encrypted tunnels as opposed to a single tunnel between the remote node and the host. Requirement 6.3.1 seems to force an interpretation of a serial chain of tunnels. An additional interpretation could be that both encryptions need to be in place via a VPN from remote host to ESP control point for strong authentication, then an SSL tunnel or some other encryption within the established tunnel would additionally be required (i.e. HTTPS inside a Cisco VPN). Any requirement that may result in an interpretation request must be reworded to remove the ambiguity.
Colt Norrish	PacifiCorp	1	Negative	Regarding the deletion of CIP-005-3 R2.4, we have no objection.  Regarding the additional material of R6, we have the following comments:  <b>R6</b> -- "Remote Access" is not defined adequately. Does Remote Access refer to "human interactive access" or does it encompass any and all network communications between a host internal to the ESP and a host external to the ESP? Is there any distinction between read only remote access and write enabled remote access? Have we abandoned the distinction between human interactive access and system to system communications?  <b>Recommendation:</b> Define "Remote Access" such that it is qualified as "human interactive access".

Voter	Entity	Segment	Vote	Comment
				<p><b>R6.1</b> -- This language indicates that only two categories of individuals may be granted remote access: employees of the entity and vendor technical support personnel. This would exclude third parties who simply need to retrieve data, but are not employees of the entity nor provide technical support. For example, Cowlitz Public Utility District is a non-operator owner of the Swift No. 2 generating facility operated by PacifiCorp, and thus currently has access privileges to the site and data. Cowlitz PUD also has some access rights to data related to the Swift No. 1 facility which is owned and operated by PacifiCorp. Under the new language in R6.1, Cowlitz PUD, as a third party entity, would lose any remote access privileges, which is problematic.</p> <p><b>Recommendation:</b> Avoid categories of personnel and simply require that all remote access comply with the principle of "least privilege" or add business partner as an attribute for qualification of remote access.</p> <p><b>R6.3</b> -- This section needs a technical feasibility exception for legacy equipment that does not support encryption. For example, telnet protocol which may well be encrypted by virtue of it's traversing a VPN between the Access Point and the VPN client, but would not be encrypted between the internal host and the Access Point.</p> <p><b>Recommendation:</b> Include the phrase, "where technically feasible".</p> <p><b>R6.4</b> -- This language needs clarification. What is meant by "communicate directly"? Specifically, at what point in the OSI stack are we inserting this "barrier" to direct communication? Layer 3 (firewall - perhaps NAT/PAT)? Layer 4-7 (proxy)?</p> <p><b>Recommendation:</b> Drop this requirement completely.</p>

Voter	Entity	Segment	Vote	Comment
Frank F. Afranji	Portland General Electric Co.	1	Negative	<p>Portland General Electric (PGE) is against the proposed revisions because they will increase uncertainty in two main areas. First, the proposed revisions would lead to increased confusion about whether CIP-005 governs machine-to-machine interactions as well as human-to-machine interactions. CIP-005-3 Requirement 2.4 applied to both machine-initiated and human-initiated access, and by removing this requirement and replacing it with the proposed Requirement 6 it appears that the Standard Drafting Team proposes to limit the scope of this standard to only human-initiated access. In particular, proposed Requirement 6.3.1 seems to be intended to only apply to human-initiated access, as the term "encrypted communications" does not specifically apply to machine-initiated access. The revision needs to make clear what types of access are covered.</p> <p>Second, the proposed wording of R6.4 is not specific enough. It is not clear what specific devices would be included in an "external system used for remote access." This could be read to include the specific computer that the remote user is operating or the remote access system that is allowing such access. In addition, the NERC definition of the term "Cyber Asset" includes any programmable electronic devices and communication networks, which makes it impossible to comply with the requirement as written. PGE believes that adopting this standard without addressing these potential area of confusion would fail NERC's burden to adopt requirements that define specific obligations.</p>

Voter	Entity	Segment	Vote	Comment
Richard J Kafka	Potomac Electric Power Co.	1	Negative	<ul style="list-style-type: none"> <li>• Suggest defining the term “remote access” (e.g. An interactive user session with a Cyber Asset within an Electronic Security Perimeter, through an identified access point, from a device external to the Electronic Security Perimeter. ).</li> <li>• CIP-005-4 R6.1.1, R6.1.2, and 6.1.3. Seem to either be a duplicate of CIP-004-R4 or an overlap at the very least. Please clarify by explaining the difference or remove if a duplication of CIP-004-R4.</li> <li>• Is CIP-005-4 R6.2 creating a need for separate controls for each separate ESP? Please clarify.</li> <li>• Multifactor authentication may not be possible for CCAs. While it is understand that CIP-005 is for access rather than CCAs, however suggest that the CIP-005-4 R6.2.1 clearly state that Multifactor Auth is required to access the ESP.</li> <li>• What impact does requiring Multifactor Auth have on CIP-007 R5.3? Does each individual part of the Multifactor Auth or the overall Multifactor Auth in total need to meet the password complexity required by CIP-007 R5.3?</li> <li>• CIP-005-4 R6.2.2 and R6.2.3 appear to duplicate existing requirements in CIP-005 R3. Please clarify by explaining the difference or remove if a duplication.</li> <li>• Please consider adding "where technically feasible" to the following requirements as drafted or rewrite requirements CIP-005-4 R6.2.2. (may require TFE for duration) and CIP-005-4 R6.4 so that TFEs are not needed.</li> <li>• Please provide additional language to CIP-005-4 R6.4 to bring clarity to this requirement as it appears to conflict with R6.3. 9. The language in R6.4 should state what is to be accomplished.</li> </ul>
Brenda L Truhe	PPL Electric Utilities Corp.	1	Negative	<p><b>General comments</b></p> <ul style="list-style-type: none"> <li>• Define the term ‘Remote Access’. Assuming ‘remote access’ is meant to be interactive remote access, define remotely as specifically as possible.</li> <li>• State that ‘Remote Access’ means interactive access and not machine to machine access. Define as specifically as possible.</li> <li>• Remote access should not include ESP to ESP communication within Registered Entities network.</li> <li>• Some of the requirements in R6.x as written may not be technically</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>feasible for all assets that are within an ESP that require the capability for remote communication.</p> <p><b>R2.4</b> Original requirement deleted. No comment.</p> <p><b>R6.1.1</b> The current wording in the proposed standard is covered by other standards. Additionally, this language could imply that vendor personnel do not need to be authorized by the asset owner. This sub-requirement should be removed.</p> <p><b>R6.1.2</b> The current requirement for list of accesses and review are covered by CIP-004 R4.1 and CIP-007 R5.1.3. This requirement is redundant and should be deleted. If this requirement remains, are separate authorized access lists required for remote access?</p> <p><b>R6.1.3</b> This requirement combines two activities together that are very different in nature. Verifying who has been given authorized access and if that access is still valid is covered in CIP-004 R4.1 and CIP-007 R5.1.3. This new requirement is requesting a verification of the technical implementation to ensure the remote access is secure which would be accomplished by a vulnerability assessment, similar to CIP-007 R8. Suggest this be a sub-requirement of R6.2 which states only authorized individuals can establish remote access to the ESP.</p> <p><b>R6.2</b> Define multi-factor authentication. This was done in a subsequent release of a draft Secure Remote Access document. Ensure this is finalized with the CIP-005 changes.</p> <p><b>R6.2.1</b> Clarify when use of multi-factor authentication is required. Multi-factor authentication is required when crossing the ESP to access a cyber asset. Is multi-factor authentication required when crossing into the Corporate</p>

Voter	Entity	Segment	Vote	Comment
				<p>Network?</p> <p><b>R6.2.2</b> Systems may not be capable of accurately, or meaningfully, tracking or providing duration of access, if at all feasible. Consider the need for this logging.</p> <p><b>R6.3.1</b> Clarify what traffic needs to be encrypted. Proposed language says 'encrypted communications between the remote node and the host inside the ESP' and there is no TFE mentioned. Not all 'hosts' inside an ESP are capable of supporting encryption. Can a TFE be taken? Clarify or rephrase to 'Provide encrypted communications between remote access points to the ESP access point, where technically feasible.'</p> <p><b>R6.3.2</b> This requirement is a design requirement which should be a sub-requirement of R6.2.1 if necessary at all depending upon the definition of multi-factor authentication.</p> <p><b>R6.4</b> The requirement as worded is very ambiguous. Is this intended to apply to remote interactive access by a human or a host-to-host communication?</p> <p>Consider an individual sitting in PSP 1 using multi-factor authentication to access a CCA system in ESP 1 in PSP 1 and the CCA system sends a transaction from ESP 1 to CCA in ESP 2 in PSP 2. Is this remote access as an individual initiated the transaction? Or not, because the system is making the connection, host to host? Would this transaction need to pass through a jump server? Or is R6.4 intended to mean an individual sitting in a remote location using multi-factor authentication to access a CCA system in ESP 1 in PSP 1? More generally, is a jump server required for traffic between all assets?</p>
Laurie Williams	Public Service Company of New Mexico	1	Negative	PNM Resources applauds the effort of the CIP-005 SAR drafting team, however we believe the proposed changes do not contribute substantively to the current version of CIP-005. We offer the following recommendations for consideration in a revised version:

Voter	Entity	Segment	Vote	Comment
				<p>Remote access requires definition within the standard. The definition should clarify if the intent is remote to the company, remote to the ESP, and should also address ESP to ESP "remote access" as well. Recommend addition of "interactive" to the definition to indicate the access covered by this modified requirement is related to human to machine remote access, not machine to machine access.</p> <p>Define multifactor either within the requirement(s) or NERC Glossary. In the absence of a definition some may argue that a username and password constitute two factors for authentication. Recommend use of, or reference to, existing terminology such as ISO, NIST or the like.</p> <p>6.1.1 and 6.1.2 are already covered in CIP-003 and CIP-004 for authorizing access and maintaining a list. These additions create confusion, and appear to be redundant to requirements elsewhere in the standards. Recommend reference to other existing requirement rather than creating new.</p> <p>6.1.1 – Use of the term "specific" implies that these requirements must be completed for each ESP rather than dealing with these as a whole where multiple ESPs exist. For example, it implies an access list must be maintained for each ESP, not a single list for multiple ESPs.</p> <p>6.2 - Include "interactive" within the term "remote access".</p> <p>6.3.1 – Encrypting through the perimeter to the end node, may prevent packet inspection as devices between the end points may not be able to inspect packets for malicious content or activity. Drafting team may consider requiring encryption to the access point of the ESP, and optionally to the node itself.</p> <p>CIP-006 R2.2 requires PSP Access control and monitoring devices be protected pursuant to CIP-005 R2 and 3, however this would remove a sub-requirement no longer applicable to PSP ACM devices. The drafting team may wish to consider whether or not this was the intent or if CIP-006 will need modification to update the reference in CIP-006 R2.2.</p>

Voter	Entity	Segment	Vote	Comment
				6.4 - Add "within an Electronic Security Perimeter" to the end of the requirement to provide clarity.
Kenneth D. Brown	Public Service Electric and Gas Co.	1	Negative	<p>Project 2010-15: Urgent Action Revisions to CIP-005-3 September, 2010 Comments to Accompany Negative Vote of the PSEG Companies</p> <ol style="list-style-type: none"> <li>1) There is no definition of remote access. There needs to be an agreed to definition. Does it include interactive, human user access? Does it include computer to computer interfaces? What about access to an intermediary that in turn talks to the ESP devices? PSEG suggests that remote access for this requirement be restricted to interactive, human user access through the ESP boundary into the ESP protected network.</li> <li>2) Also needed is a definition of multifactor authentication placed in the standard rather than rely on the supporting guide document.</li> <li>3) In R.6 it should be clarified that access controls and user lists for multiple ESPs can consist of a combined control and list for all ESPs.</li> <li>4) What does "validate the record of individuals with authorized remote access" in R6.1.2 mean? Must entities validate every access attempt or only validate the list of authorized users? Please clarify.</li> <li>5) R6.1.2/6.1.3 should be incorporated as a sub requirement for R6.2 such as: "Review the list of those authorized to remotely access Cyber Assets within an Electronic Security Perimeter at least once each calendar year, with no more than 15 months between reviews and verify that access controls implemented pursuant to Requirement R6.2 only allow access to individuals authorized for that access."</li> <li>6) R6.1.1/R6.1. should be part of R6.1 and eliminate the sub requirements Suggest it be revised to read as follows: "R6.1. Establish, implement, and document procedural controls to authorize remote access to the Electronic Security Perimeter limiting access to those Responsible Entity's personnel who have authorized electronic access to those Cyber Assets and require remote access and to vendor personnel who provide technical support of the Cyber Assets within the</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>specific Electronic Security Perimeter.”</p> <p>7) R6.2.1 should be revised to (1) require multifactor authentication for remote access to the ESP but not to access CCAs inside the ESP since the latter may not be possible to implement, or provide for a TFE and (2) provide for a TFE for logging the duration of access since that is not possible with many systems and devices.</p> <p>8) R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. It should be sufficient for the encryption to terminate at device establishing the Electronic Security Perimeter. Why does the encryption need to go all the way to the device? In some cases it may need to but there should be no general requirement that all communications within an ESP be encrypted. This requirement is too prescriptive and should be clarified to indicate it allows the encryption to end at the access point to the ESP.</p> <p>9) R6.4. Should provide for a TFE for systems or software that do not support the use or relay or proxy systems that appears to be required as now written.</p>
Catherine Koch	Puget Sound Energy, Inc.	1	Negative	<p>PSE believes the word "interactive" should be added to R6 such that it reads, R6. Remote Access Controls - If a Responsible Entity wants to grant interactive remote access.... PSE believes the word "interactive" should be added to R6.1 such that it reads, R6.1. Establish, implement, and document procedural controls that establish an authorization process for interactive remote access..... PSE believes the word "interactive" should be added to R6.2.1 such that it reads, R6.2.1. Require the use of multifactor authentication to establish interactive remote access..... PSE believes the word "interactive" should be added to R6.2.2 such that it reads, R6.2.2. Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and the time and duration of interactive remote access..... PSE believes the word "interactive" and "access" should be added to R6.3.1 such that it reads, R6.3.1. Provide encrypted communications between the interactive remote access node..... PSE requests added clarity to the intent of R6.4. PSE assumes that this means a VPN concentrator, as opposed to a Cyber Asset terminating the</p>

Voter	Entity	Segment	Vote	Comment
Tim Kelley	Sacramento Municipal Utility District	1	Negative	<p>VPN directly on itself from a non-trusted network.</p> <p>Sacramento Municipal Utility District (SMUD), while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a “Yes” vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>SMUD suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. SMUD feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define “remote access”- as “any external communication originating from or through any untrusted telecommunications infrastructure into a registered entity’s Electronic Security Perimeter(s) computer network(s).”</li> <li>2. R 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 seems to differentiate between people on that list (“authorized”) versus vendors providing support.</li> <li>3. R6.1.2 requires that the access lists be reviewed “yearly” and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</p> <p>4. R6.1.3 Also seems to be redundant with CIP-004-3 R4. SMUD views the intent of securing remote access is to ensure that we protect the communications across the untrusted communication link and that we ensure authentication, authorization and accounting of the user connecting. Establishing the access point to the ESP as the secure connection is in line with the case studies provided in the guidance document</p>
Robert Kondziolka	Salt River Project	1	Affirmative	SRP requests that clarification of the proposed requirement R6.4 be provided with examples of acceptable implementations.
Henry Delk, Jr.	SCE&G	1	Affirmative	<p>1) It is good that NERC recognizes the need for remote access by Responsible Entity personnel and by vendor personnel who provide technical support. It could be better if NERC was more descriptive about an "intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset".</p> <p>2) NERC should use the development of this revision to the standard to eliminate the need for a TFE for entities using two-factor authentication. R6 will require entities using remote access to use two factor authentication, everyone will need a TFE.</p> <p>3) There are multiple references to CIP 005-3 in CIP 005-4 (R1.4 and R5.1). Is it NERC's intention to refer to a previous version of the standard.</p> <p>4) R6.2.1 says, "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter." Similar wording appears in more than one place. Is the intention to apply the requirements only for remote access to cyber assets or for all access to the electronic security perimeter?</p> <p>5) The standard strikes an inconsistent balance between being very specific in some details and very general in others. If the intention is to</p>

Voter	Entity	Segment	Vote	Comment
				be very specific, then consideration should be given for mitigating controls. Technologies, approaches, and threats change. Utilities should have a mechanism to file an exception to any requirement provided that the alternative or mitigating control provides an equivalent level of protection.
Pawel Krupa	Seattle City Light	1	Negative	While we agree with the majority of the changes recommended by the Standard Drafting Team, we nevertheless voted negative because of Requirement 6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. First, we do not believe this requirement will effectively enhance security. Specifically, by forcing end-to-end encryption for remote communications but not for sessions that originate locally provides little security benefit if you leave internally-sourced sessions in the clear. We are unaware of any other regulatory frameworks that require end-to-end (host-to- host) encryption, including PCI and HIPAA. Normal practice is to terminate encryption at the gateway. Further, this proposal introduces key management issues and could introduce operational issues if encryption fails and connections are not possible. This model introduces more points of failure. Finally, we believe this requirement will be very difficult to accomplish on any widespread basis.
Richard Salgo	Sierra Pacific Power Co.	1	Negative	There are several problematic areas in the Standard as written for this ballot. First, the revisions in the new R6 Requirement stray too far into the prescription of "how" to comply rather than the necessary statement of the "what" of the requirement and sub-requirements. We suggest that the requirement should be limited to a statement that communications from the remote host to the access point of the ESP be protected from tampering. Several methods may exist for accomplishing this goal, but they ought not to be prescribed. We also note inconsistency between R6.1.1 and CIP-004 R4 with regard to the maintenance of lists of personnel with electronic access. Proposed R6.1.1 implies that the responsible entity need not even document and list the "vendor" personnel authorized to have remote access. On a grammatical note, the text of parent Requirement R6 begins "If a Responsible Entity wants to grant remote access to..." The use of the term "wants" is subjective and imprecise. Suggest striking "wants to" and replace such that it reads "If a Responsible Entity grants remote access to..."
Dana Cabbell	Southern	1	Negative	Please see SCE's separately filed comments.

Voter	Entity	Segment	Vote	Comment
	California Edison Co.			
Horace Stephen Williamson	Southern Company Services, Inc.	1	Negative	We are concerned that the proposed requirement does not distinguish between access needed for asset support and maintenance, which does not allow direct modification or control of the BES, and access used for remote modification or control of the BES. We are concerned that no distinction is made between interactive access by a human being and programmatic access by software used for data transfer. Programmatic access is needed as part of a good overall security design to limit the amount of interactive access needed to monitor the state of the BES. We are concerned with R6.4 that the intermediate device could also be classified as a CCA. If that is the case many support PCs could be classified as CCAs which would mean an increase in the number of CCAs and all the protective measures they are offered including CIP-006. This could mean physically securing areas that were not previously designated for CIP assets.
Larry Akens	Tennessee Valley Authority	1	Negative	<p>Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this USAR. We fully support the standards development process and all the hard work and commitment by the USAR team members. For this USAR, we have the following concerns which moved us to cast a Negative vote. General Comments:</p> <ol style="list-style-type: none"> <li>1. There isn't a clear definition of the term "remote access." Without this definition there are many ways to interpret this standard. This lack of clarification makes it very difficult to frame questions associated with these proposed new requirements. For example, is communications from a Responsible Entity's non-ESP into their ESP considered remote access? Is communications between a Responsible Entity's ESP's considered remote access, see General Comment #2? Recommendation: For the purpose of this standard define remote access something like, access originating outside any defined and trusted ESP from a remote location through a data link not controlled by the Responsible Entity, explicitly excluding all Responsible Entity's Inter-ESP communications (e.g. ESP to ESP communications) and non-ESP to ESP communications.</li> <li>2. Inter-ESP communications. Without remote access being clearly</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>defined, it isn't clear if Inter-ESP communications is considered remote access. Does this require every ESP to contain an intermediate device or system for remote access? In an environment that has multiple ESP's located on a private network can there be one access point. For example, an organization that has 50 substations that are interconnected on a private network. There is an ESP at each substation with a remote access point being centralized at a control center. Is there an expectation that communication between the control center and the substations, separate ESP's, take place over encrypted communication? Recommendation: Inter-ESP communications is outside the scope of this requirement. Communications between two defined and trusted ESP's isn't considered Remote Access. This would imply there is a "mutual trust" between ESP's owned and managed by the Responsible Entity. Specific Comments: 1. 6.1 - This requirement focuses on account management which is already addressed in other standards. Recommendation: To ensure consistency across the standards we recommend that the same verbiage in CIP-007 R5 is used in this section. 2. 6.3.1 - The way this requirements is worded makes it sound like encrypted communications must be used between the remote node and each individual device it is communicating with within the ESP. This isn't technically feasible. Recommendation: Reword the requirement to make it clear that encryption is only required between the remote node (end-user device (e.g. laptop)) and the gateway into the ESP (e.g. VPN Access Point).</p> <p>3. 6.3.1 - It is unclear if language reference to "the host" means the cyber asset within the ESP versus an intermediate device or system as described in 6.4. Recommendation: Reword 6.3.1 and 6.4 to provide more clarity.</p>
John Tolo	Tucson Electric Power Co.	1	Negative	<p>more prescriptive measures are preferred, NERC means encrypt up to ESP, allowing only remote access to the intermediary device as a jumping point. There is some comfort with that definition, but not to the host, which may not be able to be encrypted. Access to Cyber Assets or Critical Cyber Assets needs to use an intermediary system within the ESP. However, if such a system is in the ESP, it becomes a Cyber Asset which needs an intermediary system.</p>

Voter	Entity	Segment	Vote	Comment
Brandy A Dunn	Western Area Power Administration	1	Affirmative	R6.4, Page 4: "Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset." Comment: Need to define "directly communicate with a Cyber Asset" or remove 6.4; as devices directly communicating with a Cyber Asset should be part of the ESP.
Mark B Thompson	Alberta Electric System Operator	2	Negative	<p>The Alberta Electric System Operator would like clarification on the term Remote Access and the phrase "remote access to the Electronic Security Perimeter". In the proposed CIP-005-4 R6, what does the term Remote Access mean? It is not readily apparent whether this term includes interactive access (i.e. user-based), point-to-point (i.e. host-to-host without user interaction), or both. The previous version CIP-005-3 R2.4 states "external interactive access" which implies it is access originating from outside the ESP, and that it only applies to user-based communication methods - this has been removed from the new version. CIP-005-4 R6 makes reference to the term "remote access to the Electronic Security Perimeter" yet it is unclear whether this means communication originating from within, or outside of, the ESP. For example, is R6 meant to address a situation where a CCA in an ESP can remotely access a CA outside the ESP?</p> <p>R6.4 states an entity shall "Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset." The requirement is not clear as to whether this intermediate device should reside inside or outside the ESP.</p> <p>If the device resides within the ESP, then does the intermediate device itself become a Cyber Asset? If not, then this needs to be clarified, because according to R6.4 remote access to this device will also require an intermediate device, resulting in an infinite chain of intermediate devices being required.</p> <p>If the device resides outside of the ESP, then this intermediate device is not afforded the protections in R1.4 and R1.5 which would not seem to be the intent for systems providing (remote) access control. Such an approach may also lead to violations of R6.3 because the intermediate device might require additional protocols, beyond those required for remote access, to communicate with Cyber Assets within the ESP.</p>

Voter	Entity	Segment	Vote	Comment
				<p>The intent would appear to be that the intermediate device should reside within the ESP. The AESO requests that NERC clarify the intent. Should the reference to CIP-005-3 in CIP-005-4 R1.4 be amended to CIP-005-4?</p>
Kim Warren	Independent Electricity System Operator	2	Negative	<ol style="list-style-type: none"> <li>1. Please clarify the meaning of "remote access" to provide a more accurate scope for the SAR. What type of remote access? What is this SAR trying to protect against?</li> <li>2. Please explain the use of "devices" in the SAR's Brief Description instead of the defined term Cyber Asset. "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)," We believe that Cyber Asset can include smartphones like a Blackberry.</li> <li>3. The revisions to CIP-005 do not respond to the SAR's intent of end point protection. The revisions speak of protecting the Electronic Security Perimeter (ESP).</li> <li>4. We recommend that the new R6 be relocated in place of the stricken R2.3 (i.e. as part of Requirement R2 - Electronic Access Controls), since not moving R6 creates the possibility of violating two Requirements for a single infraction or double-jeopardy.</li> <li>5. Instead of "remote access" we suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP".</li> <li>6. We recommend that the language for R6 be clarified to more accurately reflect the intended scope, specifically to the following: <ul style="list-style-type: none"> <li>• CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction to R6 as it stands now. Please clarify.</li> <li>• It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose.</li> </ul> </li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>However, the sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose. The language in the version history log seems to support this view. Is that the intent? If so, we recommend that the language be in the overall R6 paragraph, not as a sub-requirement. Please clarify.</p> <p>7. We recommend removing R6.1 since it duplicates CIP-004 Requirements and creates a possible double-jeopardy.</p> <p>8. We recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</p> <p>9. There is no official definition of "multifactor authentication" as used in R6.2.1. Multifactor authentication can be technical or procedural, putting this under technical requirements implies that only technical solutions are acceptable.</p> <p>10. We recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2.</p> <p>11. We do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security.</p> <p>12. We recommend removing R6.4 because this Requirement is prescriptive, telling entities how to implement. The Requirement should identify what the target is or what is the desired end result.</p>
Kathleen Goodman	ISO New England, Inc.	2	Negative	<p>We feel compelled to vote against because we have not been privy to an implementation plan. Because this is an Urgent Action SAR, the industry did not have an opportunity to request clarification on what "remote access" to provide a more accurate scope for the SAR. Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? The updates to CIP-005 do not respond to the SAR's intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP). Recommend that the new R6 should replace the stricken R2.3 since not moving R6 creates the possibility of violating two Requirements or double-jeopardy. Recommend clarifying "remote access"</p>

Voter	Entity	Segment	Vote	Comment
				<p>in R6. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP" Recommend that the language for R6 be clarified to more accurately reflect the intended scope, specifically to the following: ? Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement. ? CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now. ? It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer. Recommend removing R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy Recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2. There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural, putting this under technical requirements implies that only technical solutions are acceptable. Recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2 Do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>

Voter	Entity	Segment	Vote	Comment
Jason L Marshall	Midwest ISO, Inc.	2	Negative	<p>While we are supportive of the drafting team's effort to address attack vectors presented by remote access through this urgent standards actions, we believe there are many issues with the draft language of the standard that need to be resolved. In particular, many of our comments address ambiguity that is created over the use of certain words and phrases in the standard that could be interpreted multiple ways.</p> <ol style="list-style-type: none"> <li>1. Several of the proposed requirements refer to other requirements. Thus, the requirements tie compliance of one requirement with another requirement. In general, this should be avoided. Requirements should stand alone and not reference other requirements.</li> <li>2. This standard does not comport with the informational filing that NERC submitted to FERC on August 10, 2009 regarding its discontinued use of sub-requirements in standards development activities.</li> <li>3. Purpose: In its current state, the "Purpose" section references standards that have not yet been approved (i.e. CIP-002-4). Last sentence should be re-written to say "Standard CIP-005-4 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."</li> <li>4. R6: Please clarify what is meant by "remote access". A definition would be helpful.</li> <li>5. R6.1: Define or clarify what is meant by "authorization process".</li> <li>6. R6.1.1: Please clarify "personnel". Does this mean only the responsible entity's employees? Are contractors or vendors included?</li> <li>7. R6.1.1: Please clarify what is meant by "authorized".</li> <li>8. R6.1.1: What is meaning/intention of using the word "specific"? Also, note that the usage of the word "specific" is not consistent through the remainder of the sub-requirements. For instance R6.1.2 does not use the word specific before ESP. Why?</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>9. R6.1.1: This sub-requirement is limiting remote access to “vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter”. Was the intention to limit who the entity can grant remote access to? Isn’t the issue that unauthorized individuals should not be remotely accessing the Cyber Assets within the ESP? If the user is authorized, this isn’t an issue.</p> <p>10. R6.1.2: Clarify what “validate” and “review” means as these two words are used here. Is this intended to be an entitlement review?</p> <p>11. R6.1.2: It is difficult to differentiate between “access” and “remote access”.</p> <p>12. R6.1.3: Please clarify “review”. Is this intended to be an entitlement review?</p> <p>13. R6.1.3: What does “verify that access controls implemented pursuant to Requirement 6.2 allow access only to individuals included in the record” mean? It seems like this requirement is more complicated than necessary. Shouldn’t requirement simply be to verify that only those individuals that are supposed to have access do have access?</p> <p>14. R6.2: Please clarify or define “authorized”.</p> <p>15. R6.2: The second use of the word “establish” seems to be the wrong fit. Suggest rewriting to “Establish, implement, and document technical controls to ensure that only authorized individuals are permitted remote access to the ESP”.</p> <p>16. R6.2: This requirement discusses “remote access to the ESP”, but the sub-requirements discuss “remote access to the cyber asset”. Shouldn’t they be consistent?</p> <p>17. R6.2.1: Please define “multifactor”.</p> <p>18. R6.2.2: Please define “monitoring” or provide clarification on what is intended.</p>

Voter	Entity	Segment	Vote	Comment
				<p>19. R6.2.2: Is logging supposed to occur at the Cyber Asset or as access passes through the ESP?</p> <p>20. R6.2.3: This requirement seems to duplicate other system logging and access point requirements. Please compare CIP-005-4R6.2.3 with CIP-007-3 R5.1.2, CIP-007-3 R6.3, CIP-007-3 R6.4, CIP-005-4 R3, CIP-005-4 R3.2, and CIP-005-4 R5.3. Suggest combining log retainment requirements to eliminate redundancy.</p> <p>21. R6.3: This requirement seems to be redundant with CIP-005-4 R3 and other requirements in CIP-007.</p> <p>22. R6.3: Suggest re-writing this sub-requirement. Why is the use of "protocols" introduced? Access points should only permit needed ports and services. Is this just referring to the protocols required for remote access?</p> <p>23. R6.3.1: The term "node" is used for the first time here. Usage of this term is ambiguous; suggest using another term that is consistent with the remaining language of the proposed requirements.</p> <p>24. R6.3.1: Suggest re-writing this sub-requirement. Define "node" as it is used in this sub-requirement. This sub-requirement implies implementing/requiring encryption for all remote access from all devices.</p> <p>25. R6.3.2: This requirement seems to overlap with R6.2.1.</p> <p>26. R6.4: We believe this requirement actually represents a technical solution. It should not be made a requirement in a standard. Standards should focus on what is required and not how to implement it. The suggested wording in this requirement focuses on how to implement it. It should not be a requirement. Furthermore, the requirement is not clear since "intermediate" is not defined and it is, thus, not clear where the requirement mandates the device should reside.</p>

Voter	Entity	Segment	Vote	Comment
Gregory Campoli	New York Independent System Operator	2	Negative	<p>NYISO believes that some elements of the standard need further clarification and many elements are already covered under other standards.</p> <p>The term "remote access" needs to be defined and clarified. For example, does the term remote access encompass all communications through the electronic security perimeter or is it limited to interactive user access through the electronic security perimeter?</p> <p>R6.1 is remarkably similar to CIP-004 R4 and is therefore redundant and unnecessary.</p> <p>R6.2, R6.2.2, and R6.2.3 are remarkably similar to CIP-007 R6 and is therefore redundant and unnecessary.</p> <p>R6.2.1 is remarkably similar to CIP-005-3 R2.4 and is therefore redundant and unnecessary if CIP-005-3 R2.4 remains unchanged.</p> <p>R6.3 is remarkably similar to CIP-007 R2 and is therefore redundant and unnecessary.</p> <p>R6.3.2 essentially repeats R6.1 and is therefore redundant and unnecessary.</p> <p>R6.4 needs further clarification on several points. The term "intermediate device or system" should be defined and clarified. For example, would the firewall that controls access to the electronic security perimeter (ESP) be considered an "intermediate device or system"? Furthermore, is the term "external system" referring to the "intermediate device or system" or some other system outside the ESP. Finally, the last part of the requirement should be clarified to read ..."does not communicate directly with a Cyber Asset inside the Electronic Security Perimeter".</p>

Voter	Entity	Segment	Vote	Comment
Tom Bowe	PJM Interconnection, L.L.C.	2	Negative	Reference R6 The following language requires revision (If a Responsible Entity wants...). The definition of "remote access" needs to be defined; also, it would be appropriate to remove "to prevent unauthorized access to its Cyber Assets". Reference R6.1 The word "Establish" needs to be defined, since it is unclear what message the author(s) is trying to convey. Reference R6.1.1 Avoid enumerating different types of personnel, thus we suggest to remove the following verbiage, "and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter". Reference R6.1.2 It should refer to CIP-004 (access should be reviewed in accordance with CIP-004 R4), instead of introducing this requirement here; also, "calendar year" should not be defined here since other CIP requirements also require "annual" activities The author should maintain consistency on "authorized personnel", if not, "individuals" should be defined in the standards Reference R6.2.1 A more detail definition of "multifactor authentication" is needed, as implementations may vary based on the definition Reference R6.2.2 This requirement should be re-phrased to represent a control and not a implementation statement. For logging the user identification, is identifying the user ID enough or do we need to define the individual that used a shared ID. Reference R6.3.1 The definition of "remote node" and "remote host" needs to be clarified (is this a cyber asset?); also, the overall meaning of communication, such as, user interactive access or application to application communication. It should also refer to the technical requirement (R6.2) and not only to the procedural control. Reference R6.4 A definition of remote access is required to properly understand this statement. The intermediate device or system might be located inside of an ESP or outside of an ESP, which depending on the definition of "remote access", different architectural approaches may need to be implemented.
Charles H Yeung	Southwest Power Pool	2	Negative	There are technical flaws in the proposed revision, specifically in R6.3, dealing with encryption from the remote node into the ESP. Other flaws include some of the logging requirements from R6.2.2 These must be addressed before we can accept the proposed changes.

Voter	Entity	Segment	Vote	Comment
Richard J. Mandes	Alabama Power Company	3	Negative	We are concerned that the proposed requirement does not distinguish between access needed for asset support and maintenance, which does not allow direct modification or control of the BES, and access used for remote modification or control of the BES. We are concerned that no distinction is made between interactive access by a human being and programmatic access by software used for data transfer. Programmatic access is needed as part of a good overall security design to limit the amount of interactive access needed to monitor the state of the BES. We are concerned with R6.4 that the intermediate device could also be classified as a CCA. If that is the case many support PCs could be classified as CCAs which would mean an increase in the number of CCAs and all the protective measures they are offered including CIP-006. This could mean physically securing areas that were not previously designated for CIP assets.
Bob Reeping	Allegheny Power	3	Negative	Allegheny Power is not voting in favor of this standard due the following significant deficiencies and issues: <ul style="list-style-type: none"> <li>1) the currently written draft is ambiguous in part because the terms External and Remote are not defined;</li> <li>2) where the standard implies differences based on the originating location of the access then additional terms "Private Network" and "Public Network or Uncontrolled Private Network" should be used where appropriate as clarification;</li> <li>3) several requirements specify a single technical solution, such as traffic encryption, rather than allowing for alternate solutions that achieve the same goal;</li> <li>4) this standard should not duplicate requirements from other standards, but rather reference those requirements.</li> </ul>
Mark Peters	Ameren Services	3	Negative	In all of R6 the term "remote access" should be changed to "interactive remote access". R6.4. should be reworded to "Implement intermediate controls such that the external system used for interactive remote access does not communicate directly with Cyber Assets critical to the operations of the BES. " Multifactor authentication needs to be defined. Our suggestion is Multifactor authentication is Authentication from more than

Voter	Entity	Segment	Vote	Comment
				one discrete source/system
Raj Rana	American Electric Power	3	Negative	<p>AEP recommends a longer Implementation Plan. Getting this implemented in a complex, multi-ESP environment while preserving reliability is a significant effort. Purchasing and implementing hardware quickly, while following procedures for change management is simply not possible in a six to nine month period and AEP feels that 12 to 18 months might be more appropriate. AEP is requesting clarity on what constitutes "remote access"? There are at least three scenarios for where the traffic originates: 1) internet, 2) corporate network, 3) another ESP. Which one(s) constitute remote access? AEP would assert that at least #3 is not "remote access" and quite possibly not #2 as well. As such, the drafting team should consider explicitly excluding hosts within a separate ESP from the remote access standard. Further, machine-to-machine ("non-interactive") access may need to be excluded from remote access, even if it involves a machine outside of the ESP. In addition, the change to CIP-005 appears to introduce unnecessary overlap with other standards and requirements. Below are some specific comments in the requirements of CIP-005. R6.1 - This text doesn't belong in CIP-005 as it is a user management issue. This requirement belongs, more properly, in CIP-004, R4. It appears to overlap, and perhaps conflict with CIP-004, R4. If you're compliant with CIP-004, R4 presumably you should be able to demonstrate compliance with CIP-005, R6.1. Demonstrating compliance twice seems unnecessary and cumbersome. R6.2 - There are significant technical issues around duration of access, and yet there is little reliability value. Proving you have the duration of access for each user access appears to be enormously time consuming and resource intensive. If there is no reliability value to tracking duration of access (and it appears there is not), we suggest that it be removed from the requirement. If it remains in the requirement, Responsible Entities will have to demonstrate compliance - and RE auditors will have to measure it. R6.3 - When and where exactly would encryption be required? Which remote access scenarios would require encryption? Is encryption to the intermediate device in R6.4 sufficient? What is the purpose of the "encryption"? Is it to preserve the confidentiality of the data? If so, why? Is it to provide data integrity? AEP would recommend striking the requirement for encryption. It's very difficult to demonstrate compliance, and appears to add little reliability value. R6.4 - At a minimum, recommend broadening the definition of intermediate device to include the</p>

Voter	Entity	Segment	Vote	Comment
				<p>Electronic Security Perimeter Access Point itself. There are many different ways to implement this security control, and as written, this requirement seems to expect a very specific technical solution. Further, for multiple ESPs, a single intermediate device should be sufficient - assuming it's within an equivalent ESP. As discussed above, ESP-to-ESP traffic should be explicitly excluded from "remote access."</p>
Steven Norris	APS	3	Affirmative	<p>AZPS Feedback to NERC SAR 2010-15</p> <p>Feedback</p> <p>AZPS generally agrees with the proposed enhancements to CIP-005-3 that resolve potential ambiguities with previous versions of this Standard. AZPS also suggests the following clarifications to further avoid unnecessary Requirement numbers and reduce potential sources of confusion.</p> <p>Suggested Modifications</p> <p>AZPS suggests that R2.4 be removed to reduce unnecessary separation of requirement numbers, as follows:</p> <p>R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) <u>which shall, at least, identify and describe:</u></p> <p><del>R2.4. The required documentation shall, at least, identify and describe:</del></p> <ul style="list-style-type: none"> <li>R2.43.1. The processes for access request and authorization.</li> <li>R2.43.2. The authentication methods.</li> <li>R2.43.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.</li> <li>R2.43.4. The controls used to secure dial-up accessible connections.</li> </ul> <p>AZPS further suggests that R6.3 and R6.4 may be confusing, as the requirements to ensure encrypted communications between the remote node and the host inside the ESP seem to conflict with the requirement to implement an intermediate communication device or system. The addition of R6.3.2 may also be confusing, as it seems unnecessary to require that</p>

Voter	Entity	Segment	Vote	Comment
				<p>these protocols support R6.1 since implementing protocols that are not compliant with R6.1 should result in a state of non-compliance. It also seems possible that R6.3.1 may result in an encrypted communication stream that reduces the ability to monitor activity at the perimeter (e.g. monitoring activity within the session, which may require access to unencrypted data) and may prove problematic as some Cyber Assets within an ESP may not support encrypted remote access protocols (e.g. RDP).</p> <p>AZPS also suggests merging R6.3 and R6.4, removing the potential conflicts and still allowing for enhanced monitoring capabilities. Suggested modifications are as follows:</p> <p><del>R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that:</del></p> <p style="padding-left: 40px;"><del>R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter.</del></p> <p style="padding-left: 40px;"><del>R6.3.2. Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1.</del></p> <p><del>R6.4. Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset</del></p> <p><u>R6.3. Implement an intermediate device or system for remote access at the Electronic Security Perimeter such that:</u></p> <p style="padding-left: 40px;"><u>R6.3.1. The external system used for remote access does not communicate directly with a Cyber Asset.</u></p> <p style="padding-left: 40px;"><u>R6.3.2. Encrypted communications are ensured between the remote node and the intermediate device.</u></p>
James V. Petrella	Atlantic City Electric Company	3	Negative	<ul style="list-style-type: none"> <li>• Suggest defining the term “remote access” (e.g. An interactive user session with a Cyber Asset within an Electronic Security Perimeter, through an identified access point, from a device external to the Electronic Security Perimeter. ).</li> <li>• CIP-005-4 R6.1.1, R6.1.2, and 6.1.3. Seem to either be a duplicate of CIP-004-R4 or an overlap at the very least. Please clarify by explaining the difference or remove if a duplication of CIP-004-R4.</li> <li>• Is CIP-005-4 R6.2 creating a need for separate controls for each</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>separate ESP? Please clarify.</p> <ul style="list-style-type: none"> <li>• Multifactor authentication may not be possible for CCAs. While it is understand that CIP-005 is for access rather than CCAs, however suggest that the CIP-005-4 R6.2.1 clearly state that Multifactor Auth is required to access the ESP.</li> <li>• What impact does requiring Multifactor Auth have on CIP-007 R5.3? Does each individual part of the Multifactor Auth or the overall Multifactor Auth in total need to meet the password complexity required by CIP-007 R5.3?</li> <li>• CIP-005-4 R6.2.2 and R6.2.3 appear to duplicate existing requirements in CIP-005 R3. Please clarify by explaining the difference or remove if a duplication.</li> <li>• Please consider adding "where technically feasible" to the following requirements as drafted or rewrite requirements CIP-005-4 R6.2.2. (may require TFE for duration) and CIP-005-4 R6.4 so that TFEs are not needed.</li> <li>• Please provide additional language to CIP-005-4 R6.4 to bring clarity to this requirement as it appears to conflict with R6.3. 9. The language in R6.4 should state what is to be accomplished.</li> </ul>
Pat G. Harrington	BC Hydro and Power Authority	3	Negative	<p>The proposed revisions should indicate "what" is required rather than "how" to comply. For example, Requirement R6.3.1 requires encryption between the remote host and the host within the Electronic Security Perimeter (ESP). The requirement should require that communications from the remote host to the access point to the ESP or intermediate device should be protected from tampering. Encryption is one method but others should be allowed if they can ensure confidentiality and integrity. The proposed standard may also cause confusion between or be inconsistent with other existing CIP standards. For example, R6.1.1 limits access to specific entities while CIP-004, R4 requires a list of authorized personnel. Lastly there is no definition of "remote access" in the proposed standard.</p>
Rebecca Berdahl	Bonneville Power Administration	3	Negative	<p>Unanimous consensus of reviewers is a 'no' vote to these changes. All felt that the proposed changes do not contribute substantively to the current version. The previous version was sufficient. Reviewers also objected to being directed on "how" to comply as opposed to "what" to be complied with. Reviewers also agreed that this draft needs a better definition of "Remote Access." For example, is it access from location external to ESP?</p>

Voter	Entity	Segment	Vote	Comment
				<p>Or, is it access from outside controlled networks but within the Responsible Entity's system? Or, is it access from a location that external to the Responsible Entity's systems altogether?</p> <p>Other than the new definition of "Annual" nothing was found to be agreeable within the proposed changes.</p> <p>Comments and Recommendations are listed below.</p> <p>The existing CIP-005-3 R2.4 makes is clear that strong procedural and technical controls must be implemented to ensure "authenticity" of the access party. In some cases, that could mean encryption. It would be helpful to have a Security Guideline for CIP-005 that gave examples of strong technical and procedural controls.</p> <p>A definition of "remote access" needs to be established.</p> <p>R6 states "...implement the following controls before granting access." It would be best to implement technical and procedural controls once to support remote access and handle granting access authorizations separately.</p> <p>R6 may conflict with the current CIP-005 R3.1 which includes the verbiage "where technically feasible." Since TFE's are not allowed in the future, shouldn't the "where technically feasible" language be deleted? The new R6 should apply to dial-up.</p> <p>R6.1 is redundant with R2.4.1 (currently R2.5.1). We understand that CIP-005-3 R2.4 and R2.5 pertain only to external user interactive access (remote user access) thru the ESP for access to one or more Cyber Assets. Access to ESP ACMs (access control and monitoring) cyber assets is address by CIP-005 R1.5. If a new CIP-005 R6 requirement to address remote access is added, then the current CIP-005-3 R2.4 and R2.5 should be deleted and included in the new R6.</p> <p>R6.1.2 and R6.1.3 are redundant and conflict with the current CIP-005 R2.5.3.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.2.2 and R6.2.3 are somewhat redundant with the current CIP-005 RCIP-005 R3.2.</p> <p>R6.4.The intermediate device or system for remote access should not be an external system.</p> <p>A suggested rewording</p> <p>R6. Remote Access Controls - To prevent unauthorized access to its Cyber Assets, where interactive access into the Electronic Security Perimeter is to be enabled, prior to granting such access the Responsible entity shall:</p> <p>R6.1. Implement and document procedural and technical controls to ensure that such access is controlled and limited to authorized personnel.</p> <p>R6.2. Restrict remote access to Electronic Security Perimeter access points to methods which support authentication controls sufficient to verify the identify and authenticity of individuals remotely accessing Cyber Assets within the Electronic Security Perimeter.</p> <p>R6.3. Provide logging of all successful and failed access attempts.</p>
Steve Alexanderson	Central Lincoln PUD	3	Negative	"Remote access" is used without providing a definition. Is remote access user initiated or machine initiated or both? For maintenance access or any purpose? The promised guidance document has not been provided to help with these questions. Balloting proceeded even though the list server remained broken following many attempts to allert Monica to the problem.
Matt Culverhouse	City of Bartow, Florida	3	Negative	Some of the requirements are vague and even possibly conflict with one another.
Michelle A Corley	Cleco Corporation	3	Affirmative	None

Voter	Entity	Segment	Vote	Comment
Bruce Krawczyk	ComEd	3	Negative	<p>Scope of the R6 section should be refined to state that these requirements only apply to user interactive access and not to system-to-system access.</p> <p>1. Requirement R6.1, Procedural Controls should be clarified in each of the three subsections to eliminate ambiguity and duplication in the requirements, in particular, as to whether the language requires separate access controls and user lists for each ESP or whether all ESPs of an operating entity can be combined. Exelon opposes the separation of ESP access into individual ESP access lists and log sets as referenced by the term "specific" in R6.1.1. Requirement R6.1.2 should be removed since the need to maintain a separate record of all individuals authorized for remote access to cyber assets within an ESP is duplicative of the CIP-004-3 R4 requirement to maintain a list of personnel with authorized cyber access. In addition, the need to validate of the record of individuals at least once each calendar year is also duplicative with CIP-007-3 R5.1.3. This additional logging requirement is also a concern since individual cyber assets are typically unable to determine if an interactive user is attempting to connect from within or outside of the ESP.</p> <p>2. Requirement R6.2, subsection R6.2.1 regarding the use of multi-factor authentication to cyber assets within ESPs must be clarified. - Exelon supports the requirement for multifactor authentication for remote access to ESP-protected cyber assets, but only to the ESP itself and not to the individual Cyber assets with in the ESP. We recognize that many of the cyber assets that are within our ESPs do not and cannot support multifactor authentication (for example, remote console terminal servers, Storage Area Network (SAN) controllers and switches, and many network routers and switches). Currently, these types of devices, from many manufacturers, do not support multifactor authentication. Requirement R6.2.2 is duplicative of the logging required in CIP-007-3 R6. If additional logging is desired then the drafting team should remove the need for logging duration of access since it is not feasible on many current systems and would require substantial effort to add that capability to existing logging and monitoring systems. It also does not appear to add substantially to the utility of the logs. Requirement R6.2.3 is duplicative of the log retention required in CIP-007-3 R6.3 &amp; R6.4.</p>

Voter	Entity	Segment	Vote	Comment
				<p>3. Requirement R6.3, encrypted communications on end-to-end connections from remote users and cyber assets within the ESP raises the same problems as the multifactor authentication requirement in R6.2. Many of the same cyber assets within Exelon ESPs do not and cannot support encrypted communications with remote users. We recommend that the R6.3.1 be amended to require encrypted communications to the ESP, not to each device within the ESP. We feel that the security posture can be more consistent with this requirement, than with the multiple exceptions that would be required for all of the devices within the ESPs that cannot support end-to-end encryption.</p> <p>4. Exelon opposes requirement R6.4 in the document as it currently exists, as it and R6.3 are mutually contradictory. Many of the applications that we currently depend on for our operations and systems management are not compatible with a relay or proxy device in the middle of the communications path and would require some degree of modification. General Comment: Many of the systems are produced, tested and installed over a period of years and changes to support major revisions to NERC CIP requirements require extensive effort, cost and time. We recommend that NERC to consider a phase-in period or the allowance of TFEs for these new requirements.</p>
Peter T Yost	Consolidated Edison Co. of New York	3	Negative	<p><b><u>CIP-005-4 Comments</u></b> - Consolidated Edison supports NPCC's comments.</p> <ul style="list-style-type: none"> <li>• An implementation plan has not been posted.</li> <li>• The SAR is too broad in its scope. The SAR should be more specific on the type of Remote Access covered.</li> <li>• Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)".</li> <li>• The updates to CIP-005 do not respond to the SAR's intent of end point protection. The updates only address access across the Electronic Security Perimeter (ESP)</li> <li>• The current R6 repeats many requirements already specified in R2. The</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>contents of R6 should be moved as a sub-requirement of R2, R2.3 being the corresponding stricken requirement. As posted, some sub-requirements of R6 result in a double jeopardy.</p> <ul style="list-style-type: none"> <li>• The term "remote access" used in R6 needs clarification. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP"</li> <li>• The language for R6 requires clarification to more accurately reflect the intended scope, specifically as follows: <ul style="list-style-type: none"> <li>o Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>o CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>o It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer.</li> </ul> </li> <li>• Requirement R6.1 should be removed: it duplicates CIP-004 Requirements, resulting in double jeopardy.</li> <li>• Requirement R6.2 should be removed: it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</li> <li>• There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural (i.e. a multifactor authentication scheme can be implemented by any mix of technical and procedural controls). By putting this under technical requirements this requirement implies that only technical solutions are acceptable.</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> <li>• Requirement R6.3 duplicates the ports and services requirements in CIP-005 R4.2: it should be removed.</li> <li>• Requiring encryption across the ESP in requirement R6.3.1 to the end-device inside the ESP is against the best practice implemented by many entities of decrypting at or immediately prior to the access point. Encrypting beyond the access point removes the visibility required for content inspection as risk mitigation control.</li> <li>• Requirement R6.4 prescribes a specific mitigation control, telling how to implement. The Requirement should be redrafted to specify the control objective and allow entities to implement the specific controls required to achieve the control objective.</li> </ul>
David A. Lapinski	Consumers Energy	3	Affirmative	<p>R6.2.1. Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter. It is our understanding that multi-factor authentication requires at least two-factor authentication and that authentication of this type involves three different types of data. 1.) Something a user knows (password), 2.) Something a user has (keycard, physical token, ID-card), 3.) Something a user is (biometrics, fingerprint). One factor authentication is easy with an appropriate user password set up being allowed. Would multiple layers of password authentication be acceptable? Providing a second form of authentication may be more difficult - for example, providing some sort of physical token to the vendors would require setting up a process to provide and maintain a token requirement. This would require additional management of the tokens and costs to provide and support tokens. If NERC would allow a predefined vendor computer with IP and MAC address to serve as "something the user has", this could provide the multi-factor authentication as well. It would be helpful if NERC would define acceptable authentication methods when the standard is published.</p>

Voter	Entity	Segment	Vote	Comment
Russell A Noble	Cowlitz County PUD	3	Affirmative	Cowlitz PUD votes affirmative, after finding the negatives to not outweigh the positive progress achieved, and in order to help advance urgent progress in cyber security concerns. However, Cowlitz PUD sees a possibility for double jeopardy with compliance to requirement R6.1.2 of CIP-005-4 as presently drafted and requirement R4 of CIP-004-3. Also, after looking at the draft guidance document "Secure Remote Access," it would appear that several important points are missing in the proposed requirement R6 such as disallowing split tunneling, and limiting remote access to only as needed functions. Increased specificity in what is desired will help clarify the true intent of the Standard. Vague verbiage in requirement R6.3.2 - "authentication controls sufficient" - seems to imply the requirement is violated after an unauthorized access event even after every possible defense measure is implemented. Possible alternate: Support two or more of the following authentication controls which discriminate against unauthorized access: allowed device identification, allowed web origination addresses, hardwired disconnect to be connected on verified phone request...
Michael R. Mayer	Delmarva Power & Light Co.	3	Negative	<ul style="list-style-type: none"> <li>• Suggest defining the term "remote access" (e.g. An interactive user session with a Cyber Asset within an Electronic Security Perimeter, through an identified access point, from a device external to the Electronic Security Perimeter. ).</li> <li>• CIP-005-4 R6.1.1, R6.1.2, and 6.1.3. Seem to either be a duplicate of CIP-004-R4 or an overlap at the very least. Please clarify by explaining the difference or remove if a duplication of CIP-004-R4.</li> <li>• Is CIP-005-4 R6.2 creating a need for separate controls for each separate ESP? Please clarify.</li> <li>• Multifactor authentication may not be possible for CCAs. While it is understand that CIP-005 is for access rather than CCAs, however suggest that the CIP-005-4 R6.2.1 clearly state that Multifactor Auth is required to access the ESP.</li> <li>• What impact does requiring Multifactor Auth have on CIP-007 R5.3? Does each individual part of the Multifactor Auth or the overall Multifactor Auth in total need to meet the password complexity required by CIP-007 R5.3?</li> <li>• CIP-005-4 R6.2.2 and R6.2.3 appear to duplicate existing requirements in CIP-005 R3. Please clarify by explaining the difference or remove if</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>a duplication.</p> <ul style="list-style-type: none"> <li>• Please consider adding "where technically feasible" to the following requirements as drafted or rewrite requirements CIP-005-4 R6.2.2. (may require TFE for duration) and CIP-005-4 R6.4 so that TFEs are not needed.</li> <li>• Please provide additional language to CIP-005-4 R6.4 to bring clarity to this requirement as it appears to conflict with R6.3. 9. The language in R6.4 should state what is to be accomplished.</li> </ul>
Kent Kujala	Detroit Edison Company	3	Negative	<p>1. The term "remote access" should be defined in the standard. Suggested definition: Remote Access - An interactive user session with a Cyber Asset within an Electronic Security Perimeter, through an identified access point, from a device external to the Electronic Security Perimeter.</p> <p>2. There are numerous occurrences of the term "remote access" that can be replaced with "Remote Access" once the definition is in place.</p> <p>3. Please remove the word "wants" from R6. Suggested language for R6: Remote Access Controls - Responsible Entities shall implement the following controls prior to allowing Remote Access.</p> <p>4. In R6.1 the word "establish" should not be repeated. Suggested language for R6.1: Establish, implement, and document procedural controls for authorization of Remote Access to the Electronic Security Perimeter that include the following.</p> <p>5. In R6.1.1 replace "Limit access" with "Limit Remote Access".</p> <p>6. In R6.1.2 "at least once each calendar year, with no more than 15 months between reviews" is an improvement over the previously used but undefined term "annual". Consider replacing "annually" in R4 and R5.1 with similar language. The word "annual" can then be removed from M4.</p> <p>7. We do not see the need to link the review specified in R6.1.3 with R6.1.2. Suggested language for R6.1.3: At least once each calendar year, with no more than 15 months between reviews, verify that access controls implemented pursuant to Requirement R6.2 allow access only to individuals included in the record.</p>

Voter	Entity	Segment	Vote	Comment
				<p>8. R6.3.1 specifies encrypted communications to the host inside the Electronic Security Perimeter. The encrypted communications should be allowed to terminate at the access point. Suggested language for R6.3.1: Provide encrypted communications between the remote node and the access point to the Electronic Security Perimeter.</p> <p>9. The language in R6.4 is too prescriptive. The standard should state what is to be accomplished not how to do it. The concept of an intermediate device should be explained in a guidance document. The purpose of the intermediate device is not clear, nor is its location i.e. inside or outside of the ESP. We interpret the intent of the requirement is to prevent the introduction of malware or other vulnerabilities. Suggested language for R6.4: Implement technical controls to ensure that the external system used for remote access does not adversely affect existing cyber security controls or introduce malicious software to Cyber Assets in the Electronic Security Perimeter.</p> <p>10. In M6 remove the word "device".</p> <p>11. Complete text of R6 with all suggested revisions:</p>
Michael F Gildea	Dominion Resources Services	3	Negative	<p>PROJECT TITLE: Project 2010-15: Urgent Action Revisions to CIP-005-3 DATE: 0 Affirmative 1 Negative 0 Abstain COMMENTS:</p> <p>Dominion believes properly authorized personnel must be allowed to provide remote operational and maintenance support for cyber assets within an Electronic Security Perimeter to maintain reliable operation of the Bulk Electric System. The application of remote access security measures should be carefully applied to avoid inadvertent, adverse reliability impacts. Several specific issues with proposed CIP-005-4 R6 changes must be addressed before the new requirement can be properly interpreted and consistently implemented throughout the industry.</p> <p>R6.1 – This requirement duplicates access control requirements addressed in CIP-005 R2 and CIP-004 R4. Dominion suggests moving requirement R6.1.1 to requirement R2 as a sub-requirement to R2.1. Requirement R6.1.2 repeats and may even contradict access authorization requirements in CIP-004 R4 regarding the review and validation of personnel with</p>

Voter	Entity	Segment	Vote	Comment
				<p>authorized cyber access to Critical Cyber Assets (e.g., quarterly access reviews vs 15 months for ESP access). Dominion suggests referring to requirement CIP-004 R4 or CIP-005 R2 (which refers to CIP-004 R4) instead of specifying separate review requirements in R6.1.2 and R6.1.3. If the requirement to validate who has remote access to an ESP once a calendar year is kept, please define a calendar year and clarify how a review is conducted 'at least once each calendar year, with no more than 15 months between reviews'.</p> <p>R6.2.1 – The deletion of existing requirement R2.3 removes the reference to 'external interactive access into the Electronic Security Perimeter'. However, the reference to multifactor authentication in this requirement suggests the term 'remote access' refers to interactive user access. Do the remote access requirements apply to remote devices that poll devices inside an ESP or data connections between multiple ESPs? The term 'remote access' should be more clearly defined.</p> <p>Based on FERC Order 706 paragraph 511, the reference to multifactor authentication is too prescriptive. That Order cited two-factor authentication and digital certificates as <i>examples</i> of strong authentication but did not specify that they were the only methods allowed.</p> <p>R6.2.2 – Dominion questions the feasibility of monitoring and logging the <i>duration</i> of remote access sessions. If this requirement remains, a Technical Feasibility Exception (TFE) should be allowed. Monitoring and logging requirements are already addressed in requirements R3 and R5 of CIP-005 and should be removed from R6.2.2 and R6.2.3.</p> <p>R6.3 – Serial connections via dial-up modems cannot support protocol/port restrictions or encrypted communications. Dial-up access is addressed in CIP-005 R2. Does CIP-005 R6 apply to dial-up access?</p> <p>R6.3.1 – According to the Purpose statement in the Introduction section of proposed standard CIP-005-4, the standard focuses on the identification and protection of the Electronic Security Perimeter (ESP) and perimeter access points. However, requirement R6.3.1 specifies encryption between a remote node and devices inside the ESP instead of between a remote node and an access point. This practice would prohibit adequate inspection at the access point to insure access has been authorized. The requirement only recognizes end-to-end encryption and does not permit the use of network level encryption.</p> <p>Encryption from a remote access point to a host inside the ESP may not be</p>

Voter	Entity	Segment	Vote	Comment
				<p>technically feasible for all device types and precludes intrusion inspection of the traffic through the access point. If this requirement stands a Technical Feasibility Exception (TFE) should be allowed.</p> <p>R6.4 - The requirement to 'implement an intermediate device or system' to communicate remotely with a cyber asset within an ESP appears to contradict requirement R6.3.1, which suggests that the remote node must communicate directly with the host using encrypted communications. (In addition, isn't the intermediate device itself a remote node?) Please define 'intermediate device or system'.</p> <p>In general, Dominion supports the following measures for remotely accessing cyber assets within an ESP:</p> <ul style="list-style-type: none"> <li>• Multifactor authentication for interactive access.</li> <li>• Introduction of an intermediate device or system so interactive access from an external device does not communicate directly with a cyber asset within an ESP.</li> <li>• Use of encryption from a remote device to an ESP access point</li> </ul> <p>Requiring that 1) anyone granted remote access to an ESP has access to protected devices inside the ESP, and 2) removal of access to all devices inside an ESP requires removal of remote access to the ESP.</p>
Henry Ernst-Jr	Duke Energy Carolina	3	Negative	<ol style="list-style-type: none"> <li>1. <b>R2.4.</b> Sub-requirement R2.4. has been deleted and R6. has been added to address remote access. Rather than remove R2.4. as a whole, and shift all the numberings for the other R2. sub-requirements, the word "<i>Deleted</i>" should appear instead. This will reduce the effort and cost of updating existing documentation.</li> <li>2. <b>R4.</b> While we find the R4. sub-requirements best practices, there is little connection between these activities and a vulnerability assessment as the term is used in the security industry. Additionally, vulnerability scan assessments often compromise the integrity of the BES. There are few cases where a generation plant can be in a complete outage to safely perform a discovery of access points. Future versions of CIP, at this time, do not include discovery of access points or review of controls for default accounts on perimeter devices. Suggest providing guidance rather than requirements for these</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>activities. Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R4.</b> Network Security Assessment - The Responsible Entity shall perform a security assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The assessment shall include, at a minimum, the following: <ul style="list-style-type: none"> <li><b>R4.1.</b> A document identifying the assessment process;</li> <li><b>R4.2.</b> A review to verify that only ports and services required for operations at these access points are enabled;</li> <li><b>R4.3.</b> <i>deleted</i></li> <li><b>R4.4.</b> A review of controls for default accounts, passwords, and network management community strings associated with the network devices that form the Electronic Security Perimeter;</li> <li><b>R4.5.</b> Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.</li> </ul> </li> </ul> <p>3. <b>R6.</b> Define remote access. A person attempting to gain access to an ESP from an external location. External remote interactive access. <b>The verbiage needs to be consistent throughout the new requirement and its sub-requirements and must</b> further clarify that interactive access is a human-to-machine connection and NOT a machine-to-machine connection. Is access "to" or "thru" the ESP? Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.</b> Remote Access Controls — Each Responsible Entity shall implement the following controls before granting remote access to Cyber Assets inside an Electronic Security perimeter from any network point outside that perimeter:</li> </ul> <p>4. <b>R6.1.</b> is redundant with CIP004 R4. Also, this requirement is not written in the language of the customer or user. The term, "procedural controls," is a military/aviation term. It means "a method of airspace control that relies on a combination of previously agreed and promulgated orders and procedures." The customer or user of these requirements is neither military nor aviation; therefore, the</p>

Voter	Entity	Segment	Vote	Comment
				<p>terminology is inappropriate and confusing. Consider using a more specific and customer understood term, such as procedure, process, policy, or something similar that clearly identifies what NERC expects the industry to produce to show compliance. There is no need to include "document" in any requirement. Any documentation would have to exist to provide evidence of compliance. We use "implement" in the suggested rewrite because it encompasses "establishing."</p> <p>Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.1.</b> Each Responsible Entity shall implement a procedure for authorizing external remote interactive access to cyber assets within the Electronic Security Perimeter.</li> </ul> <p>5. <b>R6.1.1.</b> It is not necessary to distinguish between types of personnel who have authorized electronic access. Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.1.1.</b> Each Responsible Entity shall limit external remote interactive access to only the personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter.</li> </ul> <p>6. <b>R6.1.2.</b> Each requirement should be written as a separate sentence to avoid a compound or overly complex requirement. Also, we question whether "validate" is the correct term to use here. Is "validate" the same as "review"? This requirement is very similar to, and perhaps redundant to CIP-004-3 requirements R4. and R4.1., and the term "review" is used there. Possible rewrites:</p> <ul style="list-style-type: none"> <li>• <b>R6.1.2.</b> The responsible entity shall maintain a record of individuals it authorizes to have remote access to cyber assets within its electronic security perimeters.</li> <li>• <b>R6.1.2.</b> The responsible entity shall review the record of individuals having authorized remote access at least once each calendar year, with no more than 15 months between reviews.</li> </ul> <p>7. <b>R6.1.3.</b> Suggest improved wording:</p> <ul style="list-style-type: none"> <li>• <b>R6.1.3.</b> The responsible entity shall verify that access controls allow access only to individuals it has identified in the record as authorized to remotely access cyber assets</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>within its electronic security perimeters.</p> <p>8. <b>R6.2.</b> Recommend defining the term “technical controls”. Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.2.</b> The responsible entity shall implement technical controls to ensure that only authorized individuals can establish remote access to cyber assets within its electronic security perimeters.</li> </ul> <p>9. <b>R6.2.1.</b> Ambiguous wording should be clarified. Is this requirement intended to mean that the individuals granted remote access have to use multifactor authentication or does it mean that the person authorizing the access use multifactor authentication. This requirement is prescriptive because it prescribes a specific type of technology. Can all devices support multifactor authentication? Would it be a better approach to require a particular level (for example, high, medium, low) of authentication or is that also not possible depending on what devices are in place? Does this requirement conflict with Order 706, paragraph 511? Is "multifactor authentication" synonymous with "two-factor authentication" or does it mean more than two factors? If it means more than two factors, NERC should define the term. Where there is potential for two or more interpretations of a requirement or a word or a phrase in a requirement, NERC should define or explain what it means. Possible rewrites:</p> <ul style="list-style-type: none"> <li>• <b>R6.2.1.</b> The responsible entity shall require the use of multifactor authentication by individuals who remotely access cyber assets within its electronic security perimeters.</li> <li>• <b>R6.2.1.</b> The responsible entity shall require strong authentication of individuals who remotely access cyber assets within its electronic security perimeters.</li> </ul> <p>10. <b>R6.2.2.</b> appears to be redundant with CIP-005 R3. and R5. sub-requirements. Also it is wordy and prescriptive. Does it matter whether the process is electronic or manual? If not, the words are unnecessary and make the requirement wordy. NERC can write using singular or plural words (for example, process or processes); inform</p>

Voter	Entity	Segment	Vote	Comment
				<p>the industry that the word means one or many. This will eliminate the "one or more" type phrases and the "(s)" endings on some words. Is this requirement really two requirements, one for logging; and one for monitoring? Do monitoring and logging occur at the same time or at different times? Does logging have to occur before monitoring can occur? If the latter, it should precede monitoring in the text of the requirement. If the intent is to log the remote session itself, then the requirement needs to be reworded. Possible rewrites:</p> <ul style="list-style-type: none"> <li>• <b>R6.2.2.</b> The responsible entity shall implement one or more electronic or manual processes for logging the user identification and the time of initiation of external remote interactive access to Cyber Assets within the Electronic Security Perimeter.</li> <li>• <b>R6.2.2.</b> The responsible entity shall implement processes for logging remote access to cyber assets within its electronic security perimeters.</li> <li>• <b>R6.2.2.2.</b> The log shall include the following elements: <ul style="list-style-type: none"> <li>• Identification of the individual who establishes remote access.</li> <li>• The time the remote access occurs.</li> <li>• The duration of the remote access.</li> </ul> </li> <li>• <b>R6.2.2.3.</b> The responsible entity shall implement a process for monitoring remote access to cyber assets within its electronic security perimeters.</li> </ul> <p>11. <b>R6.2.3.</b> is presently redundant with CIP 005 R5. sub-requirements. With the above changes to R6.2.2., then R6.2.3. is no longer redundant. Possible rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.2.3.</b> The responsible entity shall retain the remote access logs for a minimum of ninety calendar days or as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008.</li> </ul> <p>12. <b>R6.3.</b> needs clarification. Suggested rewrite:</p> <ul style="list-style-type: none"> <li>• <b>R6.3.</b> The responsible entity shall encrypt all communications allowed to pass through an Electronic</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>Security Perimeter access point for the purpose of remote access where they pass through portions of the network that are not within the Electronic Security Perimeter.</p> <p>13. <b>R6.3.1.</b> and <b>R6.3.2.</b> are not always feasible. It is understood from the members of the UASAR drafting team, that TFEs may not be able to be included in this version. If true, this needs to be re-worded to allow for technical limitations. Also, this may not be necessary for external remote interactive access which never leaves a trusted network. Because of R6.4., the external system used for access does not communicate directly with the Cyber Asset. It is implied that the intermediate device is in the DMZ, therefore it should be acceptable that only the communication between the external system and the intermediate device be encrypted. R6.3.2. should be deleted, and R6.3.1. should be reworded as follows:</p> <ul style="list-style-type: none"> <li>• <b>R6.3.1.</b> The responsible entity shall provide encrypted communications between the external system used for external remote interactive access and the intermediate device or system as required per R6.4.</li> </ul> <p>14. <b>R6.4.</b> What is an intermediate device? NERC may need to define this term. Could it mean a firewall, a virtual private network, or something else? Possible rewrites:</p> <ul style="list-style-type: none"> <li>• <b>R6.4.</b> The responsible entity shall implement an intermediate device or system between an external access system and a cyber asset.</li> <li>• <b>R6.4.</b> The responsible entity shall implement an intermediate device or system between an external access system and a cyber asset so that the external system does not communicate directly with the cyber asset.</li> </ul> <p>15. <b>Additional Comments</b></p> <ul style="list-style-type: none"> <li>• In some of the example rewrites, terms that NERC has defined in its glossary are not formatted with initial caps. This is because many of those terms are regular nouns, not proper nouns, and a technical writer would not ordinarily initial cap the words.</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> <li>• There are areas where the -3 in the standard number was not changed to -4. For example, see 4.2.3 under Applicability and Requirement R1.4.</li> <li>• A technical writer (not a subject matter expert who writes) should participate in the drafting and editing of all requirements. The technical writer should be present through the entire development process, not just at the end to wordsmith the requirements.</li> </ul>
Sally Witt	East Kentucky Power Coop.	3	Negative	<p>The new requirement (R6) is a good start but lacks in certain areas. First, why does R6.1.1 explicitly restrict remote access to “the Responsible Entity’s personnel” and “vendor personnel who provide technical support”? Should not the Responsible Entity determine who are appropriate to have remote access? Examples that do not fall into these two categories could include a contractor or vendor providing some kind of service other than technical support, or employees of another entity that receive SCADA services from the Responsible Entity. Second, the meaning of “remote access” is not entirely clear. This seems to be pointed only at human interactive access but does not explicitly state such. Are automated data connections such as TASE.2 data links or RTU traffic that enter the perimeter considered “remote access”? Third, there should be an exemption or other provision for traffic that originates in one ESP, passes over a secure link, and enters a second equivalent ESP (such as primary and backup control centers). This type of connection should not be forced to meet some of the requirements like multifactor authentication or an intermediate device. Finally, R6.4 seems to contradict itself. It requires that “the external system used for remote access does not communicate directly with a Cyber Asset” but the “intermediate device or system” it connects to would undoubtedly be a Cyber Asset.</p>

Voter	Entity	Segment	Vote	Comment
Kevin Querry	FirstEnergy Solutions	3	Negative	FE believes clarifications are required for the proposed standard and therefore casts a Negative vote with the following suggestions: R6.2.3 - We recommend the deletion of R6.2.3 as data retention is already covered in R5.3. Also, we do not agree that retention of information for investigations should be mandated in a reliability requirement. The retention of information for an investigation is applicable to any standard requirements as specified by the Regional Entity conducting the investigation. This is further reinforced in section 1.3.1 of the Data Retention section of the standard. R6.3.1 - We suggest rewording the requirement to "Provide encrypted communications between the remote node and the Electronic Security Perimeter access control device." We suggest this change because there is no encryption of data traffic "inside" the ESP. R6.3.2 - Requirements R6.3.2 and R6.2.1 appear duplicative. Therefore we suggest deleting R6.3.2 and rewording R6.2.1 as follows: "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter that are sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1."
Lee Schuster	Florida Power Corporation	3	Negative	<p>General comments:</p> <ul style="list-style-type: none"> <li>o A definition should be included for remote access that emphasizes human-to-machine interaction and excludes machine-to-machine and application access. We believe the emphasis on support and maintenance is key for some entities so that concept should be included in the definition. The drafting team discussed the idea used in the CIP-011 draft...something like "for the purpose of this standard...remote access is..." It was mentioned in some discussions that we do the same for "multifactor" but we believe the addition of "minimum of two-factor" is sufficient.</li> <li>o Understanding the direction to make changes in this one standard and for it to be a standalone set of requirements for secure remote access, the consensus is strongly on the side of removing the requirements that are addressed elsewhere in the CIP standards. With this feedback, we believe we need to assess the approach and decide how to remove overlap and duplicity, e.g. R6.1 Access lists, 6.2.2 monitoring/logging, etc. R6.2.1: We recommend replacing the original text with: "Require the use of multifactor authentication, with a minimum of two factor authentication, to establish</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>remote access to Cyber Assets within an Electronic Security Perimeter.” Adding “with a minimum of two factor authentication” clarifies what is required. R6.2.2: Replace “time and duration” with “login time and logout time”. This is information that most systems will be able to log. R6.3 has the following problems:</p> <ul style="list-style-type: none"> <li>o R6.3 addresses restricting protocols at access points to the ESP. Restricting protocols at ESP access points is addressed in R2 and does not need to be addressed, and should not be addressed in two different requirements.</li> <li>o R6.3.1 implies that remote access communications must encrypted end-to-end. This is technically challenging, administratively burdensome and not necessary for a secure remote access solution.</li> <li>o R6.3.2 is redundant to R6.1 - it basically states that R6.1 needs to be enforced. That is an unnecessary statement. To correct these problems, we recommend R6.3 and its sub-requirements are replaced with the following: “Implement the remote access system such that communications are encrypted whenever they traverse an unprotected network or a public data network.” Note: “Public data network” is defined in Federal Standard 1037C. R6.4: As written, this requirement is impossible - the external system must communicate with Cyber Asset. Replace “Cyber Asset” with “Critical Cyber Asset.”</li> </ul>
Anthony L Wilson	Georgia Power Company	3	Negative	<p>We are concerned that the proposed requirement does not distinguish between access needed for asset support and maintenance, which does not allow direct modification or control of the BES, and access used for remote modification or control of the BES. We are concerned that no distinction is made between interactive access by a human being and programmatic access by software used for data transfer. Programmatic access is needed as part of a good overall security design to limit the amount of interactive access needed to monitor the state of the BES. We are concerned with R6.4 that the intermediate device could also be classified as a CCA. If that is the case many support PCs could be classified as CCAs which would mean an increase in the number of CCAs and all the protective measures they are offered including CIP-006. This could mean physically securing areas that were not previously designated for CIP</p>

Voter	Entity	Segment	Vote	Comment
				assets.
Gwen S Frazier	Gulf Power Company	3	Negative	We are concerned that the proposed requirement does not distinguish between access needed for asset support and maintenance, which does not allow direct modification or control of the BES, and access used for remote modification or control of the BES. We are concerned that no distinction is made between interactive access by a human being and programmatic access by software used for data transfer. Programmatic access is needed as part of a good overall security design to limit the amount of interactive access needed to monitor the state of the BES. We are concerned with R6.4 that the intermediate device could also be classified as a CCA. If that is the case many support PCs could be classified as CCAs which would mean an increase in the number of CCAs and all the protective measures they are offered including CIP-006. This could mean physically securing areas that were not previously designated for CIP assets.
David L Kiguel	Hydro One Networks, Inc.	3	Negative	<p>Hydro One is casting a negative vote for the following reasons:</p> <ol style="list-style-type: none"> <li>7. There is no implementation plan accompanying the proposed standard.</li> <li>8. The industry did not have an opportunity to request clarification on what "remote access" means to provide a more accurate scope for the SAR. Questions such as: What type of remote access? What is this SAR trying protect? should be answered.</li> <li>9. Why the SAR's Brief Description does uses the term "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)." We believe that Cyber Assets can even include smart-phones like Blackberry.</li> <li>10. The updates to CIP-005 do not respond the SAR's intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP).</li> <li>11. We believe that the new R6 should replace the stricken R2.3 since, as written, it creates the possibility of violating two Requirements by the same event (double-jeopardy).</li> <li>12. We do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security</li> </ol> <p>In addition, we recommend the following:</p>

Voter	Entity	Segment	Vote	Comment
				<p>(h) Clarify “remote access” in R6. Instead of “remote access” suggest using “remote interactive user access to Cyber Assets in the ESP from outside of the ESP”</p> <p>(i) The language for R6 must be clarified to more accurately reflect the intended scope, specifically to the following:</p> <ul style="list-style-type: none"> <li>• Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>• The CAN-005 document appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>• It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access.</li> </ul> <p>(j) The language in the version history log needs to be clearer.</p> <p>(k) Remove R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy.</p> <p>(l) Remove R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</p> <p>(m) There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural; putting this under technical requirements implies that only technical solutions are acceptable.</p> <p>(n) Remove R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2.</p> <p>(o) Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>

Voter	Entity	Segment	Vote	Comment
Charles Locke	Kansas City Power & Light Co.	3	Negative	These proposed changes to CIP-005 are conflicting and add substantial confusion regarding the principles of remote access to Critical Cyber Assets.
Charles A. Freibert	Louisville Gas and Electric Co.	3	Negative	<p>Comments of E.ON U.S. On Negative Vote on Project 2010-15</p> <p>R6.1.2 Are the requirements stated here different from those defined in CIP-004 R4? If not, we would suggest removing this requirement.</p> <p>R6.1.3 Again, are these requirements different from those stated in the existing CIP-004 R4? If so, these differences (i.e., additional requirements) should be noted and clarified.</p> <p>R6.2 E.ON U.S. suggests adding clarification to the requirement "...to ensure only authorized individuals can establish remote access to the..." so that it reads "...to ensure only authorized individuals can establish remote, external, interactive access to the...".</p> <p>R6.2.3 Is this a change to requirement CIP-005 R5.3 regarding the retention of electronic access logs? If the requirements stated here are different, then these differences should be clarified.</p> <p>R 6.3.1 By encrypting the message all the way from the remote node to the host within the ESP the ability to detect and block malicious traffic at the access point to the ESP is removed. This would necessitate the addition of host-based intrusion detection/prevention on all assets to which remote connections are being established. Host-based protection systems are generally not as robust and effective as a single- purpose appliance for detecting and blocking the widest range of threats/ attacks. E.ON U.S. believes a better solution is to use an appliance based IPS solution on the inside of the access point prior to permitting connection to a CCA device and not requiring encryption beyond the access point.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R 6.3.2 Is this simply restating 6.1 and 6.2.1 requiring strong procedural and technical authentication controls?</p> <p>R6.4 The addition of an intermediate jump-host or proxy device actually introduces an additional set of vulnerabilities (those associated with this device) that could be attacked and compromise the Integrity of the protected ESP. Worse yet, once compromised, these could allow remote attackers access to the protected ESPs while leaving the false impression that security was actually better.</p> <p>Missing from the SAR is a clear and concise definition for "remote access". This seems to have been generally interpreted to-date as external access from outside the corporate enterprise environment. However, with CIP-011, NERC seems to be moving towards an interpretation as "any electronic access from outside the ESP". This is a significant change if that is the intent, and could require entities to make major infrastructure and procedural modifications.</p> <p>There has been much discussion over the last several months regarding the permissible use of remote access by entities. It seems NERC has been leaning towards a stance that external, interactive, remote access is permissible (given the proper controls) for administrative or maintenance support. However, this use for remote operations (with full-control capabilities) seems to not be allowed. The SAR as written does not address this point if that is the intended position, and E.ON U.S. believes the intent should be clearly stated.</p> <p>One additional note on the SAR...one of the most ambiguous requirements discussed over the past several months regarding NERC's guidance on remote access stated that the devices utilized to connect remotely must be documented and treated as CCA's. This implies that these devices must also be afforded the physical security protections (i.e., the 6-wall boundary). If this physical security requirement must be met, this effectively negates the ability for any sort of "mobile device", such as a</p>

Voter	Entity	Segment	Vote	Comment
				laptop, to be utilized outside a protected security perimeter. Despite repeated attempts to have this clarified, to-date we have been unable to get an opinion on this specific point from NERC/SERC. Without this exception, the majority of use-cases for our remote access will not be permitted, making all of these additional controls unnecessary.
Greg C Parent	Manitoba Hydro	3	Negative	<p>General Comments:</p> <ol style="list-style-type: none"> <li>1. Remote Access: It is unclear whether "remote access" refers to "remote interactive access" of a person to the Cyber Asset, or remote machine-to-machine access with the Cyber Asset. Both these types of access are distinct, and have different security solutions. If the intent is to address the person to Cyber Asset access, and the machine-to-machine Cyber Asset access, then they should be addressed separately in the standard.</li> <li>2. Removal of Technically Feasible: Legacy devices may be unable to meet the prescriptive technical requirements of the proposed R6, and therefore the requirements should only apply where technically feasible, and be subject to the Technical Feasibility Exception process.</li> <li>3. Version History: The standard applies to Cyber Assets, not Critical Assets. The reference to "for support staff maintenance" in the Action is not reflected in the accompanying SAR, which makes vague references to remote access. The proposed standard, as written, could be interpreted to apply to remote access for any purpose. R6 - The current wording is too broad. Suggest wording "The Responsible Entity shall implement the following controls before granting remote interactive access to its Electronic Security Perimeters, to prevent unauthorized access to its Cyber Assets within its Electronic Security Perimeters." R6.1.1 - Vendor personnel who provide technical support for Cyber Assets within the ESP should also be authorized. Suggest wording "... vendor personnel who have authorized electronic access who provide technical support ...". R6.2.1 - The current wording could be interpreted as requiring multifactor authentication to, and including, the Cyber Asset within the ESP. Not all Cyber Assets within the ESP will support multifactor authentication. Multifactor authentication to the ESP should be sufficient. R6.3 - The actual intent of Requirement 6.3 is unclear. Regarding the statement "Restrict the protocols ... to protocols that: Provide encrypted communications .... " Is the intent that the protocol</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>provide the encryption? Not all protocols provide encryption, although other technologies can encrypt communications, but not at the protocol level. Is the intent that the protocol support the authentication? Not all protocols support authentication, although other technologies can support authentication. The intent of the requirement should be to require secure communications, without being overly prescriptive. The terms "remote node" and "host" are not clear, are not defined, and are not used anywhere else in CIP-003 through CIP-009. R6.3.1 - Requirement 6.3.1 specifies that encrypted communications must terminate at a host within the ESP. VPN tunnels that terminate at a firewall provide the same or a better level of security as VPN tunnels that terminate at an internal proxy server, are a mainstream IT architecture and should not be excluded. This architecture also has the advantage of supporting unencrypted traffic within the ESP, which allows the firewall's anti-malware software and the IDS sensors inside the ESP to analyze the traffic. The current wording excludes this architecture. R6.4 - The wording, the intent, and the security value of Requirement 6.4 is unclear and this requirement should be removed.</p>
Don Horsley	Mississippi Power	3	Negative	<p>We are concerned that the proposed requirement does not distinguish between access needed for asset support and maintenance, which does not allow direct modification or control of the BES, and access used for remote modification or control of the BES. We are concerned that no distinction is made between interactive access by a human being and programmatic access by software used for data transfer. Programmatic access is needed as part of a good overall security design to limit the amount of interactive access needed to monitor the state of the BES. We are concerned with R6.4 that the intermediate device could also be classified as a CCA. If that is the case many support PCs could be classified as CCAs which would mean an increase in the number of CCAs and all the protective measures they are offered including CIP-006. This could mean physically securing areas that were not previously designated for CIP assets.</p>

Voter	Entity	Segment	Vote	Comment
Steven M. Jackson	Municipal Electric Authority of Georgia	3	Affirmative	As stated by MEAG Power on 9/14/10 during the Pre-Ballot Window for this proposed new standard, MEAG Power has concerns about the meaning of the current language being proposed in R6.3.1. MEAG Power is voting "yes" under the assumption that the goal of an entity providing "encrypted communications between the remote node and the host inside the Electronic Security Perimeter" could be accomplished by an entity providing encryption between the remote node and an intermediate device - so that any external system(s) used for remote access does not communicate directly with a Cyber Asset within the Electronic Security Perimeter.
Tony Eddleman	Nebraska Public Power District	3	Negative	<p>R6.2.1 Comments:</p> <ul style="list-style-type: none"> <li>Does the RSA authentication system equipment need to be on the inside of the ESP and PSP?</li> <li>Does the system (server/PC) that authenticates the remote user need to be on the inside of the ESP and PSP? For example, could a system (Windows Terminal Server or dedicated PC) on the outside of the ESP and PSP be used as a workstation that validates user authentication via multifactor authentication? The user then launches an application that then allows them to authenticate to a CCA or non-CCA without multifactor authentication but via the ESP controls limit access by IP address and port.</li> </ul> <p>R6.2.2 Comments:</p> <ul style="list-style-type: none"> <li>Is the duration of the interactive session in relationship to the first system or all subsequent systems as well? For example, I log into Non-CCA Server A. Server A is inside the ESP. It prompts me for my multifactor authentication as it is the initial system I access through the ESP. From Server A I start a remote session to CCA Server B which is not directly accessible through the ESP. Do I only need log the duration of access to Server A or do I also need to record separately the access duration to Server B?</li> </ul> <p>R6.3.1 Comments:</p> <ul style="list-style-type: none"> <li>What levels of encryption are acceptable? DES, 3DES, Blowfish, AES?</li> <li>Can a VPN tunnel be utilized between the remote node and a VPN appliance on the ESP or does the encryption have to be between the first internal host and the external host communicating into the</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>ESP?</p> <ul style="list-style-type: none"> <li>If VPN tunnels are allowed, split tunnel configurations should be disallowed.</li> </ul> <p>R6.4 Comments: This seems confusing as all devices within an ESP are either Critical Cyber Assets (CCA) or Non-Critical Cyber Assets (Non-CCA). Is this meant to say "Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a <b>Critical</b> Cyber Asset." or is this to mean that communications are required to go through a control/protection device such as a firewall or inline IDS?</p>
David Burke	Orange and Rockland Utilities, Inc.	3	Negative	<p>An implementation plan has not been posted. The SAR is too broad in its scope. The SAR should be more specific on the type of Remote Access covered. Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter),". The updates to CIP-005 do not respond to the SAR's intent of end point protection. The updates only address access across the Electronic Security Perimeter (ESP) The current R6 repeats many requirements already specified in R2. The contents of R6 should be moved as a sub-requirement of R2, R2.3 being the corresponding stricken requirement. As posted, some sub-requirements of R6 result in a double jeopardy. The term "remote access" used in R6 needs clarification. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP" The language for R6 requires clarification to more accurately reflect the intended scope, specifically as follows:</p> <ul style="list-style-type: none"> <li>o Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>o CAN-005 appears to allow remote interactive user access for operations</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</p> <p>o It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer. Requirement R6.1 should be removed: it duplicates CIP-004 Requirements, resulting in double jeopardy. Requirement R6.2 should be removed: it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2. There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural (i.e. a multifactor authentication scheme can be implemented by any mix of technical and procedural controls). By putting this under technical requirements this requirement implies that only technical solutions are acceptable. Requirement R6.3 duplicates the ports and services requirements in CIP-005 R4.2: it should be removed. Requiring encryption across the ESP in requirement R6.3.1 to the end-device inside the ESP is against the best practice implemented by many entities of decrypting at or immediately prior to the access point. Encrypting beyond the access point removes the visibility required for content inspection as risk mitigation control. Requirement R6.4 prescribes a specific mitigation control, telling how to implement. The Requirement should be redrafted to specify the control objective and allow entities to implement the specific controls required to achieve the control objective.</p>

Voter	Entity	Segment	Vote	Comment
Ballard Keith Mutters	Orlando Utilities Commission	3	Negative	<p>Draft Comments on CIP005 UA SAR We question the need for this Urgent Action SAR. The existing standard calls for strong authentication for interactive access at all access points into the ESP. As currently worded, this includes any type of remote access that this SAR is attempting to address. We believe that this SAR and the proposed changes to CIP006 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511. 511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document. FERC directed only that NERC provide additional guidance, beyond that provided in the version 1 standard and frequently asked questions, as to what constitutes "strong authentication". This could be accomplished through a guidance document, rather than a change to the standards. In order 706, FERC also clarified that its intent was not to be prescriptive, but to provide examples, and not limit authentication to specific options, which this SAR and the proposed</p>

Voter	Entity	Segment	Vote	Comment
				<p>changes to the standard would effectively do. It appears that NERC intends to restrict or curtail the practice of remotely accessing critical cyber assets within an ESP. While we agree that remote access should be secure, we believe that the ability for operational support personnel and vendors to remotely access these assets is critical to the ongoing reliable operation of the Bulk Electric System. Careful consideration must be given to avoid inadvertent adverse reliability impact through the restriction or curtailment of remote access. Beyond this issue, there are several specific problems with the proposed changes that must be addressed for this standard to be properly interpreted and consistently implemented across the industry. These include: R6 Definition of remote access. It is not clear from the SAR or the standard what is included under the definition of remote access. The SAR uses the terms "access", "secure remote access" and "external access" interchangeably. The standard only uses the term remote access, but it is not clear if that is limited to interactive access on the part of a human being, or also applies to automated access between applications or monitoring functions. For example, a log consolidation tool may connect to devices across multiple ESPs to collect log information. Vendors have read only monitoring tools which poll cyber assets connected to generating units for operational performance and and eventual tuning. It is also not clear if access between trusted ESPs over secure persistent VPN tunnels would be considered remote access. We suggest using the term "remote interactive access", with a definition of such that limits the scope of this requirement to "interactive access on the part of a human being into a NERC designated and protected ESP from a non-NERC protected network outside of that ESP such as the Internet, corporate business network, or a business partner network." R6.2.1 Requirement for multi-factor authentication. The term multi-factor authentication needs to be defined. We are interpreting that this is referring to what is commonly known as two-factor authentication. This is particularly alarming in that it prescribes a particular type of technology which entities must implement which FERC had warned against. Entities should have the option to choose what technology best meets the need in a given situation and NERC should provide examples or guidance on technologies that represent strong authentication. Entities should be allowed to implement authentication technology that is equivalent or better than multi-factor authentication from a reliability perspective that may vary from situation to situation. Additionally, in some of the examples provided</p>

Voter	Entity	Segment	Vote	Comment
				<p>above, applications are not capable of implementing this type of authentication. For ESP to ESP access across a persistent VPN tunnel, this should not even be necessary, as access originates from one secure ESP to another, and traffic is encrypted in transit. R6.2.2 Duration of remote access. Consideration should be given to the feasibility of tracking the duration of access. Not all systems will provide this functionality. R6.3.1 Encryption to the host. This requirement is not technically feasible for most equipment operating in a control system environment today including RTUs, Process Controllers, PLCs,. This equipment generally will not support encryption to the "host" level. In addition, issues such as latency and performance will need to be considered within control systems networks. Encryption of communication inside the access point may also obviate network-level intrusion detection controls that many entities have implemented. As it relates to requirement R6.4 it would appear that the "intermediate device" would be the only "remote node" allowed to access "hosts" within the Electronic Security Perimeter. Additionally, rather than use the term "host" (which we believe is new to the standards) the existing term "cyber asset" should be used. R6.4 Intermediate devices. It is not clear what the intent of this requirement is, and how it would be implemented. We assume that this is referring to a terminal services type of connection for interactive access, however that would not be feasible or necessary for application to application access or access from within another trusted ESP, or the corporate network. Also, the intermediate device itself would be considered a cyber asset used in the control or monitoring of the ESP, so the external system would still be directly connecting to a cyber asset. We would recommend rewording this to state "Implement an intermediate device or system (i.e. terminal server or other similar device) such that the external system used for remote interactive access does not communicate directly through the ESP." Additionally, this seems to conflict with requirement R6.3.1 which assumes that the remote node is communicating directly with the "host" (cyber asset) within the perimeter. R6.1 Access Lists - This requirement and associated sub-requirements appear to be redundant to the requirements of CIP004 R4. The CIP004 requirement already calls for a review of lists of personnel with authorized cyber or physical access to</p>

Voter	Entity	Segment	Vote	Comment
John Apperson	PacifiCorp	3	Negative	<p>Regarding the deletion of CIP-005-3 R2.4, we have no objection.</p> <p>Regarding the additional material of R6, we have the following comments:</p> <p><b>R6</b> -- "Remote Access" is not defined adequately. Does Remote Access refer to "human interactive access" or does it encompass any and all network communications between a host internal to the ESP and a host external to the ESP? Is there any distinction between read only remote access and write enabled remote access? Have we abandoned the distinction between human interactive access and system to system communications?</p> <p><b>Recommendation:</b> Define "Remote Access" such that it is qualified as "human interactive access".</p> <p><b>R6.1</b> -- This language indicates that only two categories of individuals may be granted remote access: employees of the entity and vendor technical support personnel. This would exclude third parties who simply need to retrieve data, but are not employees of the entity nor provide technical support. For example, Cowlitz Public Utility District is a non-operator owner of the Swift No. 2 generating facility operated by PacifiCorp, and thus currently has access privileges to the site and data. Cowlitz PUD also has some access rights to data related to the Swift No. 1 facility which is owned and operated by PacifiCorp. Under the new language in R6.1, Cowlitz PUD, as a third party entity, would lose any remote access privileges, which is problematic.</p> <p><b>Recommendation:</b> Avoid categories of personnel and simply require that all remote access comply with the principle of "least privilege" or add business partner as an attribute for qualification of remote access.</p> <p><b>R6.3</b> -- This section needs a technical feasibility exception for legacy equipment that does not support encryption. For example, telnet protocol which may well be encrypted by virtue of it's traversing a VPN between the</p>

Voter	Entity	Segment	Vote	Comment
				<p>Access Point and the VPN client, but would not be encrypted between the internal host and the Access Point.</p> <p><b>Recommendation:</b> Include the phrase, "where technically feasible".</p> <p><b>R6.4</b> -- This language needs clarification. What is meant by "communicate directly"? Specifically, at what point in the OSI stack are we inserting this "barrier" to direct communication? Layer 3 (firewall - perhaps NAT/PAT)? Layer 4-7 (proxy)?</p> <p><b>Recommendation:</b> Drop this requirement completely.</p>
Michael Mertz	PNM Resources	3	Negative	<p>PNM Resources applauds the effort of the CIP-005 SAR drafting team, however we believe the proposed changes do not contribute substantively to the current version of CIP-005. We offer the following recommendations for consideration in a revised version:</p> <p>Remote access requires definition within the standard. The definition should clarify if the intent is remote to the company, remote to the ESP, and should also address ESP to ESP "remote access" as well. Recommend addition of "interactive" to the definition to indicate the access covered by this modified requirement is related to human to machine remote access, not machine to machine access.</p> <p>Define multifactor either within the requirement(s) or NERC Glossary. In the absence of a definition some may argue that a username and password constitute two factors for authentication. Recommend use of, or reference to, existing terminology such as ISO, NIST or the like.</p> <p>6.1.1 and 6.1.2 are already covered in CIP-003 and CIP-004 for authorizing access and maintaining a list. These additions create confusion, and appear to be redundant to requirements elsewhere in the standards. Recommend reference to other existing requirement rather than creating new.</p> <p>6.1.1 – Use of the term "specific" implies that these requirements must be completed for each ESP rather than dealing with these as a whole where multiple ESPs exist. For example, it implies an access list must be</p>

Voter	Entity	Segment	Vote	Comment
				<p>maintained for each ESP, not a single list for multiple ESPs.</p> <p>6.2 - Include “interactive” within the term “remote access”.</p> <p>6.3.1 – Encrypting through the perimeter to the end node, may prevent packet inspection as devices between the end points may not be able to inspect packets for malicious content or activity. Drafting team may consider requiring encryption to the access point of the ESP, and optionally to the node itself.</p> <p>CIP-006 R2.2 requires PSP Access control and monitoring devices be protected pursuant to CIP-005 R2 and 3, however this would remove a sub-requirement no longer applicable to PSP ACM devices. The drafting team may wish to consider whether or not this was the intent or if CIP-006 will need modification to update the reference in CIP-006 R2.2.</p> <p>6.4 - Add “within an Electronic Security Perimeter” to the end of the requirement to provide clarity.</p>
Sam Waters	Progress Energy Carolinas	3	Negative	<p><b>General comments:</b></p> <ul style="list-style-type: none"> <li>• A definition should be included for remote access that emphasizes human-to-machine interaction and excludes machine-to-machine and application access. We believe the emphasis on support and maintenance is key for some entities so that concept should be included in the definition. The drafting team discussed the idea used in the CIP-011 draft...something like “for the purpose of this standard...remote access is...” It was mentioned in some discussions that we do the same for “multifactor” but we believe the addition of “minimum of two-factor” is sufficient.</li> <li>• Understanding the direction to make changes in this one standard and for it to be a standalone set of requirements for secure remote access, the consensus is strongly on the side of removing the requirements that are addressed elsewhere in the CIP standards. With this feedback, we believe we need to assess the approach and decide how to remove overlap and duplicity, e.g. R6.1 Access lists, 6.2.2 monitoring/logging, etc.</li> </ul> <p><b>R6.2.1:</b> We recommend replacing the original text with:</p>

Voter	Entity	Segment	Vote	Comment
				<p>“Require the use of multifactor authentication, with a minimum of two factor authentication, to establish remote access to Cyber Assets within an Electronic Security Perimeter.”</p> <p>Adding “with a minimum of two factor authentication” clarifies what is required.</p> <p><b>R6.2.2:</b> Replace “time and duration” with “login time and logout time”. This is information that most systems will be able to log.</p> <p>R6.3 has the following problems:</p> <ul style="list-style-type: none"> <li>• R6.3 addresses restricting protocols at access points to the ESP. Restricting protocols at ESP access points is addressed in R2 and does not need to be addressed, and should not be addressed in two different requirements.</li> <li>• R6.3.1 implies that remote access communications must encrypted end-to-end. This is technically challenging, administratively burdensome and not necessary for a secure remote access solution.</li> <li>• R6.3.2 is redundant to R6.1 – it basically states that R6.1 needs to be enforced. That is an unnecessary statement.</li> </ul> <p>To correct these problems, we recommend R6.3 and its sub-requirements are replaced with the following:</p> <p style="padding-left: 40px;">“Implement the remote access system such that communications are encrypted whenever they traverse an unprotected network or a public data network.”</p> <p>Note: “Public data network” is defined in Federal Standard 1037C.</p> <p><b>R6.4:</b> As written, this requirement is impossible – the external system must communicate with Cyber Asset. Replace “Cyber Asset” with “Critical Cyber Asset.”</p>

Voter	Entity	Segment	Vote	Comment
Jeffrey Mueller	Public Service Electric and Gas Co.	3	Negative	<p>1) There is no definition of remote access. There needs to be an agreed to definition. Does it include interactive, human user access? Does it include computer to computer interfaces? What about access to an intermediary that in turn talks to the ESP devices? PSEG suggests that remote access for this requirement be restricted to interactive, human user access through the ESP boundary into the ESP protected network.</p> <p>2) Also needed is a definition of multifactor authentication placed in the standard rather than rely on the supporting guide document.</p> <p>3) In R.6 it should be clarified that access controls and user lists for multiple ESPs can consist of a combined control and list for all ESPs.</p> <p>4) What does "validate the record of individuals with authorized remote access" in R6.1.2 mean? Must entities validate every access attempt or only validate the list of authorized users? Please clarify.</p> <p>5) R6.1.2/6.1.3 should be incorporated as a sub requirement for R6.2 such as: "Review the list of those authorized to remotely access Cyber Assets within an Electronic Security Perimeter at least once each calendar year, with no more than 15 months between reviews and verify that access controls implemented pursuant to Requirement R6.2 only allow access to individuals authorized for that access."</p> <p>6) R6.1.1/R6.1. should be part of R6.1 and eliminate the sub requirements Suggest it be revised to read as follows: "R6.1. Establish, implement, and document procedural controls to authorize remote access to the Electronic Security Perimeter limiting access to those Responsible Entity's personnel who have authorized electronic access to those Cyber Assets and require remote access and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter."</p> <p>7) R6.2.1 should be revised to (1) require multifactor authentication for remote access to the ESP but not to access CCAs inside the ESP since the latter may not be possible to implement, or provide for a TFE and (2) provide for a TFE for logging the duration of access since that is not possible with many systems and devices.</p>

Voter	Entity	Segment	Vote	Comment
				<p>8) R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. It should be sufficient for the encryption to terminate at device establishing the Electronic Security Perimeter. Why does the encryption need to go all the way to the device? In some cases it may need to but there should be no general requirement that all communications within an ESP be encrypted. This requirement is too prescriptive and should be clarified to indicate it allows the encryption to end at the access point to the ESP.</p> <p>9) R6.4. Should provide for a TFE for systems or software that do not support the use or relay or proxy systems that appears to be required as now written.</p>
James Leigh-Kendall	Sacramento Municipal Utility District	3	Negative	<p>Sacramento Municipal Utility District (SMUD), while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a “Yes” vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>SMUD suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. SMUD feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define “remote access”- as “any external communication originating from or through any untrusted telecommunications infrastructure into a registered entity’s Electronic Security</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>Perimeter(s) computer network(s)."</p> <ol style="list-style-type: none"> <li>2. R 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> <li>3. R6.1.2 requires that the access lists be reviewed "yearly" and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</li> <li>4. R6.1.3 Also seems to be redundant with CIP-004-3 R4. SMUD views the intent of securing remote access is to ensure that we protect the communications across the untrusted communication link and that we ensure authentication, authorization and accounting of the user connecting. Establishing the access point to the ESP as the secure connection is in line with the case studies provided in the guidance document</li> </ol>
Scott Peterson	San Diego Gas & Electric	3	Negative	<p>R6. Need to clearly define what is meant by "remote access". Is it as broad as anything outside the ESP?</p> <p>R6.1.1 Suggested language change to make consistent with other CIP standards: "Limit access to only the Responsible Entity's personnel and their contractors and service vendors who have authorized cyber access to Cyber Assets within the specific Electronic Security Perimeter."</p> <p>R6.1.2: Does this require a separate list of personnel with authorized remote access? How does this fit with CIP007 R5.1.3?</p> <p>R6.1.3: This would be better placed under 6.2 to simplify and make easier to understand.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.2: Suggested language change to be more consistent with the other CIP requirements, "only authorized individuals" should be changed to "only authorized personnel".</p> <p>R6.2.1: Suggested language change: Change "multifactor" to "two or more forms of authentication" to avoid confusion.</p> <p>R6.2.2: Suggested language changes: Change "electronic" to "automatic".</p> <p>R6.2.3: This is already required by CIP007 and CIP008 and could lead to multiple violations for the same event. It doesn't add any additional security and should be removed from this standard.</p> <p>R6.3: Suggested language change: Change "protocols" to "routable protocols". Question: What does NERC define as protocols for the purpose of remote access?</p> <p>R6.3.1: Question - Couldn't this requirement present additional security concerns given the IPS/IDS system would be unable to inspect encrypted packets?</p> <p>R6.3.2: Question- Wouldn't this be better placed under R6.1? This seems overly confusing to keep referencing other requirements.</p> <p>R6.4: Suggested change to language: Change "Cyber Asset" to "Cyber Asset within the ESP". Question - What does "external system" mean? Is it external to the ESP? Is it external to the entity's network?</p>

Voter	Entity	Segment	Vote	Comment
Dana Wheelock	Seattle City Light	3	Negative	<p>While we agree with the majority of the changes recommended by the Standard Drafting Team, we nevertheless voted negative because of Requirement 6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. First, we do not believe this requirement will effectively enhance security. Specifically, by forcing end-to-end encryption for remote communications but not for sessions that originate locally provides little security benefit if you leave internally-sourced sessions in the clear. We are unaware of any other regulatory frameworks that require end-to-end (host-to- host) encryption, including PCI and HIPAA. Normal practice is to terminate encryption at the gateway. Further, this proposal introduces key management issues and could introduce operational issues if encryption fails and connections are not possible. This model introduces more points of failure. Finally, we believe this requirement will be very difficult to accomplish on any widespread basis.</p>
Travis Metcalfe	Tacoma Public Utilities	3	Negative	<p>Tacoma Power supports the development of this Standard and is of the opinion that the draft implementation guidelines provided by NERC offers best security practices and sound architectural solutions that would mitigate the security issues the revised CIP-005-4 Standard seeks to address.</p> <p>While we have read and appreciate the technical concerns raised by other entities, Tacoma Power supports APPA's position that the draft implementation guidelines provided by NERC offer a solution intended to protect BES critical cyber assets from a real vulnerability of Virtual Private Networks ("VPNs") that is known by federal agencies to have in fact been exploited.</p> <p>Unfortunately, Tacoma Power, while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a "Yes" vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p>

Voter	Entity	Segment	Vote	Comment
				<p>Tacoma Power suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. Tacoma Power feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define "remote access".</li> <li>2. 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 Seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> <li>3. 6.1.2 requires that the access lists be reviewed "yearly" and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</li> <li>4. 6.1.3 Also seems to be redundant with CIP-004-3 R4.</li> </ol> <p>Thank you for your consideration in this matter.</p>

Voter	Entity	Segment	Vote	Comment
Ronald L Donahey	Tampa Electric Co.	3	Negative	<p>We question the need for this Urgent Action SAR. The existing standard calls for strong authentication for external interactive access at all access points into the ESP. As currently worded, this includes any type of remote access that this SAR attempts to address. We believe that this SAR and the proposed changes to CIP005 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511. "511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document." FERC directed only that NERC provide additional guidance, beyond that provided in the version 1 standard and frequently asked questions, as to what constitutes "strong authentication". This could be accomplished through a guidance document, or the addition of a definition for "strong authentication" to the NERC glossary of terms, rather than a change to the standards. In order 706, FERC also clarified that its intent was not to be prescriptive, but to provide examples, and not limit</p>

Voter	Entity	Segment	Vote	Comment
				<p>authentication to specific options, which this SAR and the proposed changes to the standard would effectively do. Furthermore, we believe that the term “external interactive access into the Electronic Security Perimeter” already includes remote access as intended by this SAR. If this term lacks sufficient clarity to be consistently interpreted by the industry, we would recommend the addition of a definition of “external interactive access” to the NERC glossary of terms. If this urgent action SAR is truly required, there are several specific problems with the proposed changes that must be addressed for this standard to be properly interpreted and consistently implemented across the industry. These include: R6 Definition of remote access. It is not clear from the SAR or the standard what is included under the definition of remote access. The SAR uses the terms “access”, “secure remote access” and “external access” interchangeably. The standard only uses the term remote access, but it is not clear if that is limited to interactive access on the part of a human being, or if it also applies to automated access between applications or monitoring functions. For example, a log consolidation tool may connect to devices across multiple ESPs to collect log information. Vendors have “read only” monitoring tools which poll cyber assets connected to generating units for operational performance and eventual tuning. It is also not clear if access between trusted ESPs over secure persistent VPN tunnels would be considered remote access. We suggest using the term “remote interactive access”, with a definition of such that limits the scope of this requirement to “interactive access on the part of a human being into a NERC designated and protected ESP from a non-NERC protected network outside of that ESP such as the Internet, corporate business network, or a business partner network.” R6.2.1 Requirement for multi-factor authentication. The term multi-factor authentication needs to be defined. We are interpreting that this is referring to what is commonly known as two-factor authentication. This is particularly alarming in that it prescribes a particular type of technology which entities must implement which FERC had warned against. Entities should have the option to choose what technology best meets the need in a given situation and NERC should provide examples or guidance on technologies that represent strong authentication. Entities should be allowed to implement authentication technology that is equivalent or better than multi-factor authentication from a reliability perspective that may vary from situation to situation. Additionally, in some of the examples provided</p>

Voter	Entity	Segment	Vote	Comment
				<p>above, applications are not capable of implementing this type of authentication. For ESP to ESP access across a persistent VPN tunnel, this should not even be necessary, as access originates from one secure ESP to another, and traffic is encrypted in transit. R6.2.2 Duration of remote access. Consideration should be given to the feasibility of tracking the duration of access. Not all systems will provide this functionality. R6.3.1 Encryption to the host. This requirement is not technically feasible for most equipment operating in a control system environment today including Remote Terminal Units (RTUs), and Programmable Logic Controllers, (PLCs). This equipment generally will not support encryption to the "host" level. In addition, issues such as latency and performance will need to be considered within control systems networks. Encryption of communication inside the access point may also obviate network-level intrusion detection controls that many entities have implemented. As it relates to requirement R6.4 it would appear that the "intermediate device" would be the only "remote node" allowed to access "hosts" within the Electronic Security Perimeter. Additionally, rather than use the term "host" (which we believe is new to the standards) the existing term "cyber asset" should be used. R6.4 Intermediate devices. It is not clear what the intent of this requirement is, and how it would be implemented. We assume that this is referring to a terminal services type of connection for interactive access; however that would not be feasible or necessary for application to application access or access from within another trusted ESP, or the corporate network. Also, the intermediate device itself would be considered a cyber asset used in the control or monitoring of the ESP, so the external system would still be directly connecting to a cyber asset. We would recommend rewording this to state "Implement an intermediate device or system (i.e. terminal server or other similar device) such that the external system used for remote interactive access does not communicate directly through the ESP." Additionally, this seems to conflict with requirement R6.3.1 which assumes that the remote node is communicating directly with the "host" (cyber asset) within the perimeter. R6.1 Access Lists - This requirement and associated sub-requirements appear to be redundant to the requirements of CIP004 R4. The CIP004 requirement already calls for a review of lists of personnel with authorized cyber or physical access to cyber ass</p>
Ian S Grant	Tennessee	3	Negative	Tennessee Valley Authority (TVA) appreciates the opportunity to comment

Voter	Entity	Segment	Vote	Comment
	Valley Authority			<p>on this USAR. We fully support the standards development process and all the hard work and commitment by the USAR team members. For this USAR, we have the following concerns which moved us to cast a Negative vote. General Comments:</p> <p>1. There isn't a clear definition of the term "remote access." Without this definition there are many ways to interpret this standard. This lack of clarification makes it very difficult to frame questions associated with these proposed new requirements. For example, is communications from a Responsible Entity's non-ESP into their ESP considered remote access? Is communications between a Responsible Entity's ESP's considered remote access, see General Comment #2? Recommendation: For the purpose of this standard define remote access something like, access originating outside any defined and trusted ESP from a remote location through a data link not controlled by the Responsible Entity, explicitly excluding all Responsible Entity's Inter-ESP communications (e.g. ESP to ESP communications) and non-ESP to ESP communications.</p> <p>2. Inter-ESP communications. Without remote access being clearly defined, it isn't clear if Inter-ESP communications is considered remote access. Does this require every ESP to contain an intermediate device or system for remote access? In an environment that has multiple ESP's located on a private network can there be one access point. For example, an organization that has 50 substations that are interconnected on a private network. There is an ESP at each substation with a remote access point being centralized at a control center. Is there an expectation that communication between the control center and the substations, separate ESP's, take place over encrypted communication? Recommendation: Inter-ESP communications is outside the scope of this requirement. Communications between two defined and trusted ESP's isn't considered Remote Access. This would imply there is a "mutual trust" between ESP's owned and managed by the Responsible Entity. Specific Comments:</p> <p>1. 6.1 - This requirement focuses on account management which is already addressed in other standards. Recommendation: To ensure consistency across the standards we recommend that the same verbiage in CIP-007 R5 is used in this section.</p>

Voter	Entity	Segment	Vote	Comment
				<p>2. 6.3.1 - The way this requirements is worded makes it sound like encrypted communications must be used between the remote node and each individual device it is communicating with within the ESP. This isn't technically feasible. Recommendation: Reword the requirement to make it clear that encryption is only required between the remote node (end-user device (e.g. laptop)) and the gateway into the ESP (e.g. VPN Access Point).</p> <p>3. 6.3.1 - It is unclear if language reference to "the host" means the cyber asset within the ESP versus an intermediate device or system as described in 6.4. Recommendation: Reword 6.3.1 and 6.4 to provide more clarity.</p>
James R. Keller	Wisconsin Electric Power Marketing	3	Negative	<p>The proposed standard revision contains many requirements for security specific to certain types of connections and uses, but is lacking clarity on defining those situations and where each specific requirement applies. In order to provide the sufficient guidance, the revised standard should include specific use cases to describe the requirements for, at a minimum: Accessing a Critical Cyber Asset interactively "Locally." (e.g. directly at the device) Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, but within the corporate enterprise network. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, and outside of the corporate enterprise network. Accessing a Critical Cyber Asset interactively from a different ESP. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset in a disaster recovery scenario or disaster recovery test. Accessing a Critical Cyber Asset using a computer, or programmatically from within an ESP. Accessing a Critical Cyber Asset using a computer, or programmatically from outside the ESP that contains the Critical Cyber Asset. The industry would be aided by the provision of theoretical network diagrams within the guidance to depict the interactive access options. For requirement 6, definitions should be developed for: Remote external, interactive access, and Multifactor authentication Ideally the resulting definitions should be integrated closely with the use case guidance requested above. The following suggested wordings are provided for requirements 6 through 6.4 to provide clarity and actionable direction: R6.1. Establish, implement, and document procedural controls that establish an authorization process for remote external, interactive access to the Electronic Security Perimeter that include</p>

Voter	Entity	Segment	Vote	Comment
				<p>the following. R6.1.1. Limit access to only the Responsible Entity's personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter. R6.1.2. Maintain a record of all individuals authorized for remote access to Cyber Assets within an Electronic Security Perimeter, and validate the record of individuals with authorized remote access at least once each calendar year, with no more than 15 months between reviews. R6.1.3. As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls implemented pursuant to Requirement R6.2 allow access only to individuals included in the record. R6.2. Establish, implement, and document technical controls to ensure that only authorized individuals can establish remote interactive access to the Electronic Security Perimeter. R6.2.1. Require the use of multifactor authentication to establish remote interactive access to Cyber Assets within an Electronic Security Perimeter. R6.2.2. Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and where technically feasible, log the time and duration of remote access to Cyber Assets within the Electronic Security Perimeter. R6.2.3. Retain all logs specified in Requirement R6.2.2 for a minimum of ninety calendar days, or as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008. R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that: R6.3.1. Provide encrypted communications between the remote node and the Electronic Security Perimeter. R6.3.2. Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1. R6.4. Where technically feasible , Implement an intermediate device or system such that the external system used for remote interactive access does not communicate directly with a Cyber Asset.</p>

Voter	Entity	Segment	Vote	Comment
Timothy Beyrle	City of New Smyrna Beach Utilities Commission	4	Negative	The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too proscriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security.
David Frank Ronk	Consumers Energy	4	Affirmative	R6.2.1. Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter. It is our understanding that multi-factor authentication requires at least two-factor authentication and that authentication of this type involves three different types of data. <ol style="list-style-type: none"> <li>1.) Something a user knows (password),</li> <li>2.) Something a user has (keycard, physical token, ID-card),</li> <li>3.) Something a user is (biometrics, fingerprint).</li> </ol> One factor authentication is easy with an appropriate user password set up being allowed. Would multiple layers of password authentication be acceptable? Providing a second form of authentication may be more difficult - for example, providing some sort of physical token to the vendors would require setting up a process to provide and maintain a token requirement. This would require additional management of the tokens and costs to provide and support tokens. If NERC would allow a predefined vendor computer with IP and MAC address to serve as "something the user has", this could provide the multi-factor authentication as well. It would be helpful if NERC would define acceptable authentication methods when the standard is published.
Rick Syring	Cowlitz County PUD	4	Affirmative	Cowlitz PUD votes affirmative, after finding the negatives to not outweigh the positive progress achieved, and in order to help advance urgent progress in cyber security concerns. However, Cowlitz PUD sees a possibility for double jeopardy with compliance to requirement R6.1.2 of CIP-005-4 as presently drafted and requirement R4 of CIP-004-3. Also, after looking at the draft guidance document "Secure Remote Access," it

Voter	Entity	Segment	Vote	Comment
				<p>would appear that several important points are missing in the proposed requirement R6 such as disallowing split tunneling, and limiting remote access to only as needed functions. Increased specificity in what is desired will help clarify the true intent of the Standard. Vague verbiage in requirement R6.3.2 - "authentication controls sufficient" - seems to imply the requirement is violated after an unauthorized access event even after every possible defense measure is implemented. Possible alternate: Support two or more of the following authentication controls which discriminate against unauthorized access: allowed device identification, allowed web origination addresses, hardwired disconnect to be connected on verified phone request...</p>
Frank Gaffney	Florida Municipal Power Agency	4	Negative	<p>The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too proscriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security.</p>
Thomas W. Richards	Fort Pierce Utilities Authority	4	Negative	<p>The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too prescriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security. Also, Requirement 6.3.1 could be in direct contradiction to requirement 6.4 if encryption between a remote node and a host node is interpreted to be a serial chain of encrypted tunnels as opposed to a single tunnel between the remote node and the host. Requirement 6.3.1 seems to force an interpretation of a</p>

Voter	Entity	Segment	Vote	Comment
				serial chain of tunnels. An additional interpretation could be that both encryptions need to be in place via a VPN from remote host to ESP control point for strong authentication, then an SSL tunnel or some other encryption within the established tunnel would additionally be required (i.e. HTTPS inside a Cisco VPN).
Guy Andrews	Georgia System Operations Corporation	4	Negative	<p>Comments are duplicated from Georgia Transmission Corporation. The draft standard for CIP-005-4 lays out requirements that are technically impossible (encryption to the host, R6.3.1) for GTC in some scenarios, but does not allow for a TFE. R6.3.1 is not consistent with best practices. Best practices dictate that all encrypted tunnels be terminated outside of an ESP or at the access point to the ESP such that an intrusion detection system (IDS) can inspect the traffic at the ingress point. Remote access is not defined. This standard could possibly extend to machine-to-machine interactions which would make this standard impossible to implement. Remote access is limited by R6.1.1 for only "technical support" purposes. The purpose of accessing devices remotely should not be limited by the standard. The standard does not sufficiently allow for vendors to access systems remotely for the purpose of support. At times, vendor access to systems is critical and you are unable to determine who that individual may be prior to calling a vendor's support line (i.e. Cisco). Multifactor authentication is undefined. This term needs more clarity in order for entities to reasonably understand how to meet compliance. There is a lack of clarity on R6.1.1 which indicates limiting access to personnel who have "authorized electronic access." CIP-004 R4 requires that a list be kept for personnel who have "authorized cyber access." Are these different lists? What exactly is the difference or are they equivalent? Why were different words chosen? R6.4 requires that access be provided through an intermediate device, but does not provide clarity on how this intermediate device must be managed. Does the intermediate device or system required in R6.4 become a Critical Cyber Asset? Must this system reside inside the ESP with the CCA it is providing access to, does it have to reside in its own ESP, or is it not required to reside in an ESP? Does this system fall under the requirements of CIP-005 R1.5?</p>

Voter	Entity	Segment	Vote	Comment
Christopher Plante	Integrus Energy Group, Inc.	4	Negative	<p>1) NERC needs to define Remote Access. A suggestion would be "If a Responsible Entity wants to grant human interactive external remote access..."</p> <p>2) The new requirement contains many sub-requirements which all but one are addressed in other controls. For example: The new 6.1.1 control is covered in CIP004 under access controls. Since this change is being made in CIP005, the suggestion would be to only include the technical aspect of the requirement and not all the other monitoring pieces.</p> <p>3) The new requirement 6.4 is the only piece of what's been changed that is trying to get at the technical concern, but it's too gray and needs clarification. The real technical crux of the issue is not being addressed. For example: If the threat of remote access is protect against an attacker coming thru an encrypted VPN which can't be monitored then the standard should state that responsibilities must secure and monitor that this doesn't happen.</p> <p>4) Other than adding a new requirement to address the technical concern, as mentioned in comment #3, I'm not sure how all the extra sub-requirements are providing any additional security or reliability to the BES systems.</p>
Richard Comeaux	LaGen	4	Negative	<p>I do not see where this mentions anything about restricting support personnel from being able to perform certain actions, such as control. This should have addressed that. EMS system support personnel can always use tools to manipulate database parameters, allowing themselves control ability. They all have DB tools that are needed to manipulate systems in times of emergency support. If they wanted vendors to address this, and lock it down, they should have covered it.</p>

Voter	Entity	Segment	Vote	Comment
Joseph G. DePoorter	Madison Gas and Electric Co.	4	Negative	As written in the recently approved SMP a requirement shall identify "What functional entity shall do what under what conditions to achieve what reliability objective." (page 5) Then page 6 states; Requirement: An explicit statement that identifies the functional entity responsible, the action or outcome that must be achieved, any conditions achieving the action or outcome, and the reliability-related benefit of the action or outcome. Upon review of R6, it appears that most of the sub requirements explain the "how" and not the what. Plus the word "restrict" in R6.3 is very hard to measure, it falls into the same category of the word "coordinate", used in other Standards. Within R6 the term "Remote Access Control" is not distinguished from any other form of access other than by the adjective "remote." Any and all forms of communication from outside to inside the electronic security perimeter could conceivably be regarded as "remote." Remote node is undefined. Since in R6.4, a responsible entity is required to use an "intermediate device or system", it is unclear whether the remote node is the "intermediate device or system" or the initiating system.
Douglas Hohlbaugh	Ohio Edison Company	4	Negative	FE believes clarifications are required for the proposed standard and therefore casts a Negative vote with the following suggestions: R6.2.3 - We recommend the deletion of R6.2.3 as data retention is already covered in R5.3. Also, we do not agree that retention of information for investigations should be mandated in a reliability requirement. The retention of information for an investigation is applicable to any standard requirements as specified by the Regional Entity conducting the investigation. This is further reinforced in section 1.3.1 of the Data Retention section of the standard. R6.3.1 - We suggest rewording the requirement to "Provide encrypted communications between the remote node and the Electronic Security Perimeter access control device." We suggest this change because there is no encryption of data traffic "inside" the ESP. R6.3.2 - Requirements R6.3.2 and R6.2.1 appear duplicative. Therefore we suggest deleting R6.3.2 and rewording R6.2.1 as follows: "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter that are sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1."
Mike Ramirez	Sacramento Municipal Utility District	4	Negative	Sacramento Municipal Utility District (SMUD), while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a "Yes" vote at this time due to

Voter	Entity	Segment	Vote	Comment
				<p>a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>SMUD suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. SMUD feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define "remote access"- as "any external communication originating from or through any untrusted telecommunications infrastructure into a registered entity's Electronic Security Perimeter(s) computer network(s)."</li> <li>2. R 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> <li>3. R6.1.2 requires that the access lists be reviewed "yearly" and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>4. R6.1.3 Also seems to be redundant with CIP-004-3 R4. SMUD views the intent of securing remote access is to ensure that we protect the communications across the untrusted communication link and that we ensure authentication, authorization and accounting of the user connecting. Establishing the access point to the ESP as the secure connection is in line with the case studies provided in the guidance document</p>
Hao Li	Seattle City Light	4	Negative	<p>While we agree with the majority of the changes recommended by the Standard Drafting Team, we nevertheless voted negative because of Requirement 6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. First, we do not believe this requirement will effectively enhance security. Specifically, by forcing end-to-end encryption for remote communications but not for sessions that originate locally provides little security benefit if you leave internally-sourced sessions in the clear. We are unaware of any other regulatory frameworks that require end-to-end (host-to- host) encryption, including PCI and HIPAA. Normal practice is to terminate encryption at the gateway. Further, this proposal introduces key management issues and could introduce operational issues if encryption fails and connections are not possible. This model introduces more points of failure. Finally, we believe this requirement will be very difficult to accomplish on any widespread basis.</p>
Steven R Wallace	Seminole Electric Cooperative, Inc.	4	Negative	<p>The meaning of "remote access" is ambiguous as used Access lists, logging and monitoring and retention are redundant to CIP-004 R4, CIP-005 R3. Technical feasibility must be considered. Depending on intended meaning of remote access and system architecture, the requirements for multifactor authentication and encryption may be infeasible.</p>
Keith Morisette	Tacoma Public Utilities	4	Negative	<p>Tacoma Power supports the development of this Standard and is of the opinion that the draft implementation guidelines provided by NERC offers best security practices and sound architectural solutions that would mitigate the security issues the revised CIP-005-4 Standard seeks to address.</p> <p>While we have read and appreciate the technical concerns raised by other entities, Tacoma Power supports APPA's position that the draft implementation guidelines provided by NERC offer a solution intended to protect BES critical cyber assets from a real vulnerability of Virtual Private</p>

Voter	Entity	Segment	Vote	Comment
				<p>Networks (“VPNs”) that is known by federal agencies to have in fact been exploited.</p> <p>Unfortunately, Tacoma Power, while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a “Yes” vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>Tacoma Power suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. Tacoma Power feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define “remote access”.</li> <li>2. 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 Seems to differentiate between people on that list (“authorized”) versus vendors providing support.</li> <li>3. 6.1.2 requires that the access lists be reviewed “yearly” and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>timelines and expectations outlined elsewhere in the CIP Standards</p> <p>4. 6.1.3 Also seems to be redundant with CIP-004-3 R4.</p> <p>Thank you for your consideration in this matter.</p>
Anthony Jankowski	Wisconsin Energy Corp.	4	Negative	<p>The proposed standard revision contains many requirements for security specific to certain types of connections and uses, but is lacking clarity on defining those situations and where each specific requirement applies. In order to provide the sufficient guidance, the revised standard should include specific use cases to describe the requirements for, at a minimum:</p> <ol style="list-style-type: none"> <li>1. Accessing a Critical Cyber Asset interactively "Locally." (e.g. directly at the device)</li> <li>2. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, but within the corporate enterprise network.</li> <li>3. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, and outside of the corporate enterprise network.</li> <li>4. Accessing a Critical Cyber Asset interactively from a different ESP.</li> <li>5. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset in a disaster recovery scenario or disaster recovery test.</li> <li>6. Accessing a Critical Cyber Asset using a computer, or programmatically from within an ESP.</li> <li>7. Accessing a Critical Cyber Asset using a computer, or programmatically from outside the ESP that contains the Critical Cyber Asset.</li> </ol> <p>The industry would be aided by the provision of theoretical network diagrams within the guidance to depict the interactive access options.</p> <p>For requirement 6, definitions should be developed for:</p> <ul style="list-style-type: none"> <li>• Remote external, interactive access, and</li> <li>• Multifactor authentication</li> </ul> <p>Ideally the resulting definitions should be integrated closely with the use case guidance requested above.</p>

Voter	Entity	Segment	Vote	Comment
				<p>The following suggested wordings are provided for requirements 6 through 6.4 to provide clarity and actionable direction:</p> <ul style="list-style-type: none"> <li><b>R6.1.</b> Establish, implement, and document procedural controls that establish an authorization process for remote external, interactive access to the Electronic Security Perimeter that include the following. <ul style="list-style-type: none"> <li><b>R6.1.1.</b> Limit access to only the Responsible Entity's personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter.</li> <li><b>R6.1.2.</b> Maintain a record of all individuals authorized for remote access to Cyber Assets within an Electronic Security Perimeter, and validate the record of individuals with authorized remote access at least once each calendar year, with no more than 15 months between reviews.</li> <li><b>R6.1.3.</b> As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls implemented pursuant to Requirement R6.2 allow access only to individuals included in the record.</li> </ul> </li> <li><b>R6.2.</b> Establish, implement, and document technical controls to ensure that only authorized individuals can establish remote interactive access to the Electronic Security Perimeter. <ul style="list-style-type: none"> <li><b>R6.2.1.</b> Require the use of multifactor authentication to establish remote interactive access to Cyber Assets within an Electronic Security Perimeter.</li> </ul> </li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p><b>R6.2.2.</b> Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and where technically feasible, log the time and duration of remote access to Cyber Assets within the Electronic Security Perimeter.</p> <p><b>R6.2.3.</b> Retain all logs specified in Requirement R6.2.2 for a minimum of ninety calendar days, or as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008.</p> <p><b>R6.3.</b> Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that:</p> <p><b>R6.3.1.</b> Provide encrypted communications between the remote node and the Electronic Security Perimeter.</p> <p><b>R6.3.2.</b> Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1.</p> <p><b>R6.4.</b> Where technically feasible , Implement an intermediate device or system such that the external system used for remote interactive access does not communicate directly with a Cyber Asset.</p>
Brock Ondayko	AEP Service Corp.	5	Negative	<p>AEP recommends a longer Implementation Plan. Getting this implemented in a complex, multi-ESP environment while preserving reliability is a significant effort. Purchasing and implementing hardware quickly, while following procedures for change management is simply not possible in a six to nine month period and AEP feels that 12 to 18 months might be more appropriate. AEP is requesting clarity on what constitutes "remote access"? There are at least three scenarios for where the traffic originates: 1) internet, 2) corporate network, 3) another ESP. Which one(s) constitute remote access? AEP would assert that at least #3 is not "remote access"</p>

Voter	Entity	Segment	Vote	Comment
				<p>and quite possibly not #2 as well. As such, the drafting team should consider explicitly excluding hosts within a separate ESP from the remote access standard. Further, machine-to-machine ("non-interactive") access may need to be excluded from remote access, even if it involves a machine outside of the ESP. In addition, the change to CIP-005 appears to introduce unnecessary overlap with other standards and requirements. Below are some specific comments in the requirements of CIP-005. R6.1 - This text doesn't belong in CIP-005 as it is a user management issue. This requirement belongs, more properly, in CIP-004, R4. It appears to overlap, and perhaps conflict with CIP-004, R4. If you're compliant with CIP-004, R4 presumably you should be able to demonstrate compliance with CIP-005, R6.1. Demonstrating compliance twice seems unnecessary and cumbersome. R6.2 - There are significant technical issues around duration of access, and yet there is little reliability value. Proving you have the duration of access for each user access appears to be enormously time consuming and resource intensive. If there is no reliability value to tracking duration of access (and it appears there is not), we suggest that it be removed from the requirement. If it remains in the requirement, Responsible Entities will have to demonstrate compliance - and RE auditors will have to measure it. R6.3 - When and where exactly would encryption be required? Which remote access scenarios would require encryption? Is encryption to the intermediate device in R6.4 sufficient? What is the purpose of the "encryption"? Is it to preserve the confidentiality of the data? If so, why? Is it to provide data integrity? AEP would recommend striking the requirement for encryption. It's very difficult to demonstrate compliance, and appears to add little reliability value. R6.4 - At a minimum, recommend broadening the definition of intermediate device to include the Electronic Security Perimeter Access Point itself. There are many different ways to implement this security control, and as written, this requirement seems to expect a very specific technical solution. Further, for multiple ESPs, a single intermediate device should be sufficient - assuming it's within an equivalent ESP. As discussed above, ESP-to-ESP traffic should be explicitly excluded from "remote access."</p>

Voter	Entity	Segment	Vote	Comment
Mel Jensen	APS	5	Affirmative	<p>AZPS Feedback to NERC SAR 2010-15</p> <p>Feedback</p> <p>AZPS generally agrees with the proposed enhancements to CIP-005-3 that resolve potential ambiguities with previous versions of this Standard. AZPS also suggests the following clarifications to further avoid unnecessary Requirement numbers and reduce potential sources of confusion.</p> <p>Suggested Modifications</p> <p>AZPS suggests that R2.4 be removed to reduce unnecessary separation of requirement numbers, as follows:</p> <p>R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s) <u>which shall, at least, identify and describe:</u></p> <p><del>R2.4. The required documentation shall, at least, identify and describe:</del></p> <ul style="list-style-type: none"> <li>R2.4.1. The processes for access request and authorization.</li> <li>R2.4.2. The authentication methods.</li> <li>R2.4.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.</li> <li>R2.4.4. The controls used to secure dial-up accessible connections.</li> </ul> <p>AZPS further suggests that R6.3 and R6.4 may be confusing, as the requirements to ensure encrypted communications between the remote node and the host inside the ESP seem to conflict with the requirement to implement an intermediate communication device or system. The addition of R6.3.2 may also be confusing, as it seems unnecessary to require that these protocols support R6.1 since implementing protocols that are not compliant with R6.1 should result in a state of non-compliance. It also seems possible that R6.3.1 may result in an encrypted communication stream that reduces the ability to monitor activity at the perimeter (e.g. monitoring activity within the session, which may require access to unencrypted data) and may prove problematic as some Cyber Assets within</p>

Voter	Entity	Segment	Vote	Comment
				<p>an ESP may not support encrypted remote access protocols (e.g. RDP).</p> <p>AZPS also suggests merging R6.3 and R6.4, removing the potential conflicts and still allowing for enhanced monitoring capabilities. Suggested modifications are as follows:</p> <p><del>R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that:</del></p> <p style="padding-left: 40px;"><del>R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter.</del></p> <p style="padding-left: 40px;"><del>R6.3.2. Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1.</del></p> <p><del>R6.4. Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset</del></p> <p><u>R6.3. Implement an intermediate device or system for remote access at the Electronic Security Perimeter such that:</u></p> <p style="padding-left: 40px;"><u>R6.3.1. The external system used for remote access does not communicate directly with a Cyber Asset.</u></p> <p style="padding-left: 40px;"><u>R6.3.2. Encrypted communications are ensured between the remote node and the intermediate device.</u></p>
Clement Ma	BC Hydro and Power Authority	5	Negative	<p>The proposed revisions should indicate "what" is required rather than "how" to comply. For example, Requirement R6.3.1 requires encryption between the remote host and the host within the Electronic Security Perimeter (ESP). The requirement should require that communications from the remote host to the access point to the ESP or intermediate device should be protected from tampering. Encryption is one method but others should be allowed if they can ensure confidentiality and integrity. The proposed standard may also cause confusion between or be inconsistent with other existing CIP standards. For example, R6.1.1 limits access to specific entities while CIP-004, R4 requires a list of authorized personnel. Lastly there is no definition of "remote access" in the proposed standard.</p>

Voter	Entity	Segment	Vote	Comment
George Tatar	Black Hills Corp	5	Negative	<p>Req 6: Move to follow Req 2; plus definition of "remote access" isn't clear and isn't defined anywhere in standard. Req 6.1.2: change to "annually"</p> <p>Req 6.2.1: The implementation &amp; maintenance for this requirement regarding vendors would be difficult to implement &amp; manage, as well as creating risk in response time for support. Would suggest alternate wording to multifactor, multilayer, or other strong authentication mechanisms.</p>
Francis J. Halpin	Bonneville Power Administration	5	Negative	<p>BPA is in support of the new definition of "Annual".</p> <p>The existing CIP-005-3 R2.4 makes is clear that strong procedural and technical controls must be implemented to ensure "authenticity" of the access party. In some cases, that could mean encryption. It would be helpful to have a Security Guideline for CIP-005 that gave examples of strong technical and procedural controls.</p> <p>A definition of "remote access" needs to be established.</p> <p>R6 states "...implement the following controls before granting access." It would be best to implement technical and procedural controls once to support remote access and handle granting access authorizations separately.</p> <p>R6 may conflict with the current CIP-005 R3.1 which includes the verbiage "where technically feasible." Since TFE's are not allowed in the future, shouldn't the "where technically feasible" language be deleted? The new R6 should apply to dial-up.</p> <p>R6.1 is redundant with R2.4.1 (currently R2.5.1). We understand that CIP-005-3 R2.4 and R2.5 pertain only to external user interactive access (remote user access) thru the ESP for access to one or more Cyber Assets. Access to ESP ACMS (access control and monitoring) cyber assets is address by CIP-005 R1.5. If a new CIP-005 R6 requirement to address remote access is added, then the current CIP-005-3 R2.4 and R2.5 should be deleted and included in the new R6.</p> <p>R6.1.2 and R6.1.3 are redundant and conflict with the current CIP-005 R2.5.3.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.2.2 and R6.2.3 are somewhat redundant with the current CIP-005 RCIP-005 R3.2.</p> <p>R6.4.The intermediate device or system for remote access should not be an external system.</p> <p><b>A suggested rewording</b></p> <p><b>R6.</b> Remote Access Controls — To prevent unauthorized access to its Cyber Assets, where interactive access into the Electronic Security Perimeter is to be enabled, prior to granting such access the Responsible entity shall:</p> <p><b>R6.1.</b> Implement and document procedural and technical controls to ensure that such access is controlled and limited to authorized personnel.</p> <p><b>R6.2.</b> Restrict remote access to Electronic Security Perimeter access points to methods which support authentication controls sufficient to verify the identify and authenticity of individuals remotely accessing Cyber Assets within the Electronic Security Perimeter.</p> <p><b>R6.3.</b> Provide logging of all successful and failed access attempts.</p>
Max Emrick	City of Tacoma, Department of Public Utilities, Light Division, dba Tacoma Power	5	Negative	<p>Tacoma Power supports the development of this Standard and is of the opinion that the draft implementation guidelines provided by NERC offers best security practices and sound architectural solutions that would mitigate the security issues the revised CIP-005-4 Standard seeks to address.</p> <p>While we have read and appreciate the technical concerns raised by other entities, Tacoma Power supports APPA's position that the draft implementation guidelines provided by NERC offer a solution intended to protect BES critical cyber assets from a real vulnerability of Virtual Private Networks ("VPNs") that is known by federal agencies to have in fact been exploited.</p> <p>Unfortunately, Tacoma Power, while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a "Yes" vote at this time due to a lack of definition of key</p>

Voter	Entity	Segment	Vote	Comment
				<p>elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p> <p>Tacoma Power suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. Tacoma Power feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define "remote access".</li> <li>2. 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 Seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> <li>3. 6.1.2 requires that the access lists be reviewed "yearly" and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</li> <li>4. 6.1.3 Also seems to be redundant with CIP-004-3 R4.</li> </ol> <p>Thank you for your consideration in this matter.</p>
Stephanie Huffman	Cleco Power	5	Affirmative	None

Voter	Entity	Segment	Vote	Comment
Wilket (Jack) Ng	Consolidated Edison Co. of New York	5	Negative	<p><b><u>CIP-005-4 Comments</u></b> - Consolidated Edison supports NPCC's comments.</p> <ul style="list-style-type: none"> <li>• An implementation plan has not been posted.</li> <li>• The SAR is too broad in its scope. The SAR should be more specific on the type of Remote Access covered.</li> <li>• Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)".</li> <li>• The updates to CIP-005 do not respond to the SAR's intent of end point protection. The updates only address access across the Electronic Security Perimeter (ESP)</li> <li>• The current R6 repeats many requirements already specified in R2. The contents of R6 should be moved as a sub-requirement of R2, R2.3 being the corresponding stricken requirement. As posted, some sub-requirements of R6 result in a double jeopardy.</li> <li>• The term "remote access" used in R6 needs clarification. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP"</li> <li>• The language for R6 requires clarification to more accurately reflect the intended scope, specifically as follows: <ul style="list-style-type: none"> <li>○ Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>○ CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>○ It is not clear whether requirement R6 is intended to</li> </ul> </li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer.</p> <ul style="list-style-type: none"> <li>• Requirement R6.1 should be removed: it duplicates CIP-004 Requirements, resulting in double jeopardy.</li> <li>• Requirement R6.2 should be removed: it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</li> <li>• There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural (i.e. a multifactor authentication scheme can be implemented by any mix of technical and procedural controls). By putting this under technical requirements this requirement implies that only technical solutions are acceptable.</li> <li>• Requirement R6.3 duplicates the ports and services requirements in CIP-005 R4.2: it should be removed.</li> <li>• Requiring encryption across the ESP in requirement R6.3.1 to the end-device inside the ESP is against the best practice implemented by many entities of decrypting at or immediately prior to the access point. Encrypting beyond the access point removes the visibility required for content inspection as risk mitigation control.</li> <li>• Requirement R6.4 prescribes a specific mitigation control, telling how to implement. The Requirement should be redrafted to specify the control objective and allow entities to implement the specific controls required to achieve the control objective.</li> </ul>
Amir Y Hammad	Constellation Power Source Generation, Inc.	5	Negative	<p>NERC should revise the proposed standards to clarify the remote access requirements do not apply to communication between Electronic Security Perimeters (ESP). Imposing the proposed remote access controls to communications in between ESPs would reduce effectiveness of existing security controls, assuming that remote access between ESPs could be installed. Additionally, system reliability could be affected if remote access</p>

Voter	Entity	Segment	Vote	Comment
				<p>between ESPs reduces availability of CCAs. R6.1.3: Since 6.1.2 establishes the record of individuals with authorized remote access and is referenced, the concluding phrase is unnecessary. Proposed edit: R6.1.3 As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls are implemented pursuant to Requirement R6.2. R6.2.2: Please clarify that the trigger of user logging occurs at the ESP level. Proposed edit: R6.2.2 Implement and document one or more electronic or manual processes for monitoring and logging user identification, and the time and duration of remote access through the Electronic Security Perimeter. R6.3: This requirement is repetitive and unnecessary. R3 and R6.1 already cover the requirements in R6.3. R6.4: Please clarify the intent of this requirement. It does not seem feasible to prevent direct communication with a Cyber Asset. Proposed edit: R6.4 Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Critical Cyber Asset.</p>
James B Lewis	Consumers Energy	5	Affirmative	<p>R6.2.1. Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter. It is our understanding that multi-factor authentication requires at least two-factor authentication and that authentication of this type involves three different types of data. 1.) Something a user knows (password), 2.) Something a user has (keycard, physical token, ID-card), 3.) Something a user is (biometrics, fingerprint). One factor authentication is easy with an appropriate user password set up being allowed. Would multiple layers of password authentication be acceptable? Providing a second form of authentication may be more difficult - for example, providing some sort of physical token to the vendors would require setting up a process to provide and maintain a token requirement. This would require additional management of the tokens and costs to provide and support tokens. If NERC would allow a predefined vendor computer with IP and MAC address to serve as "something the user has", this could provide the multi-factor authentication as well. It would be helpful if NERC would define acceptable authentication methods when the standard is published.</p>
Bob Essex	Cowlitz County PUD	5	Affirmative	<p>Cowlitz PUD votes affirmative, after finding the negatives to not outweigh the positive progress achieved, and in order to help advance urgent progress in cyber security concerns. However, Cowlitz PUD sees a possibility for double jeopardy with compliance to requirement R6.1.2 of</p>

Voter	Entity	Segment	Vote	Comment
				<p>CIP-005-4 as presently drafted and requirement R4 of CIP-004-3. Also, after looking at the draft guidance document "Secure Remote Access," it would appear that several important points are missing in the proposed requirement R6 such as disallowing split tunneling, and limiting remote access to only as needed functions. Increased specificity in what is desired will help clarify the true intent of the Standard. Vague verbiage in requirement R6.3.2 - "authentication controls sufficient" - seems to imply the requirement is violated after an unauthorized access event even after every possible defense measure is implemented. Possible alternate: Support two or more of the following authentication controls which discriminate against unauthorized access: allowed device identification, allowed web origination addresses, hardwired disconnect to be connected on verified phone request...</p>

Voter	Entity	Segment	Vote	Comment
Mike Garton	Dominion Resources, Inc.	5	Negative	<p>Dominion believes properly authorized personnel must be allowed to provide remote operational and maintenance support for cyber assets within an Electronic Security Perimeter to maintain reliable operation of the Bulk Electric System. The application of remote access security measures should be carefully applied to avoid inadvertent, adverse reliability impacts. Several specific issues with proposed CIP-005-4 R6 changes must be addressed before the new requirement can be properly interpreted and consistently implemented throughout the industry.</p> <p>R6.1 - This requirement duplicates access control requirements addressed in CIP-005 R2 and CIP-004 R4. Dominion suggests moving requirement R6.1.1 to requirement R2 as a sub-requirement to R2.1. Requirement R6.1.2 repeats and may even contradict access authorization requirements in CIP-004 R4 regarding the review and validation of personnel with authorized cyber access to Critical Cyber Assets (e.g., quarterly access reviews vs 15 months for ESP access). Dominion suggests referring to requirement CIP-004 R4 or CIP-005 R2 (which refers to CIP-004 R4) instead of specifying separate review requirements in R6.1.2 and R6.1.3.</p> <p>If the requirement to validate who has remote access to an ESP once a calendar year is kept, please define a calendar year and clarify how a review is conducted 'at least once each calendar year, with no more than 15 months between reviews'.</p> <p>R6.2.1 - The deletion of existing requirement R2.3 removes the reference to 'external interactive access into the Electronic Security Perimeter'. However, the reference to multifactor authentication in this requirement suggests the term 'remote access' refers to interactive user access. Do the remote access requirements apply to remote devices that poll devices inside an ESP or data connections between multiple ESPs? The term 'remote access' should be more clearly defined.</p>

Voter	Entity	Segment	Vote	Comment
Kenneth Dresner	FirstEnergy Solutions	5	Negative	Comments FE believes clarifications are required for the proposed standard and therefore casts a Negative vote with the following suggestions: R6.2.3 - We recommend the deletion of R6.2.3 as data retention is already covered in R5.3. Also, we do not agree that retention of information for investigations should be mandated in a reliability requirement. The retention of information for an investigation is applicable to any standard requirements as specified by the Regional Entity conducting the investigation. This is further reinforced in section 1.3.1 of the Data Retention section of the standard. R6.3.1 - We suggest rewording the requirement to "Provide encrypted communications between the remote node and the Electronic Security Perimeter access control device." We suggest this change because there is no encryption of data traffic "inside" the ESP. R6.3.2 - Requirements R6.3.2 and R6.2.1 appear duplicative. Therefore we suggest deleting R6.3.2 and rewording R6.2.1 as follows: "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter that are sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1."
David Schumann	Florida Municipal Power Agency	5	Negative	The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too proscriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security.
Daniel Duff	Liberty Electric Power LLC	5	Negative	My concern is the language of R6.2: "Establish, implement, and document technical controls to ensure that only authorized individuals can establish remote access to the Electronic Security Perimeter." As this reads, an entity is in violation if an unauthorized individual establishes remote access, no matter how well the Cyber Asset is defended. Malicious actions by a disgruntled employee, access granted under duress, and errors in securing passcodes are examples of acts beyond the control of the entity. Suggested change: R6.2. Establish, implement, and document technical

Voter	Entity	Segment	Vote	Comment
				controls designed to eliminate unauthorized remote access to the Electronic Security Perimeter."
Charlie Martin	Louisville Gas and Electric Co.	5	Negative	<p>Comments of E.ON U.S. On Negative Vote on Project 2010-15</p> <p>R6.1.2 Are the requirements stated here different from those defined in CIP-004 R4? If not, we would suggest removing this requirement.</p> <p>R6.1.3 Again, are these requirements different from those stated in the existing CIP-004 R4? If so, these differences (i.e., additional requirements) should be noted and clarified.</p> <p>R6.2 E.ON U.S. suggests adding clarification to the requirement "...to ensure only authorized individuals can establish remote access to the..." so that it reads "...to ensure only authorized individuals can establish remote, external, interactive access to the...".</p> <p>R6.2.3 Is this a change to requirement CIP-005 R5.3 regarding the retention of electronic access logs? If the requirements stated here are different, then these differences should be clarified.</p> <p>R 6.3.1 By encrypting the message all the way from the remote node to the host within the ESP the ability to detect and block malicious traffic at the access point to the ESP is removed. This would necessitate the addition of host-based intrusion detection/prevention on all assets to which remote connections are being established. Host-based protection systems are generally not as robust and effective as a single- purpose appliance for detecting and blocking the widest range of threats/ attacks. E.ON U.S. believes a better solution is to use an appliance based IPS solution on the inside of the access point prior to permitting connection to a CCA device and not requiring encryption beyond the access point.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R 6.3.2 Is this simply restating 6.1 and 6.2.1 requiring strong procedural and technical authentication controls?</p> <p>R6.4 The addition of an intermediate jump-host or proxy device actually introduces an additional set of vulnerabilities (those associated with this device) that could be attacked and compromise the Integrity of the protected ESP. Worse yet, once compromised, these could allow remote attackers access to the protected ESPs while leaving the false impression that security was actually better.</p> <p>Missing from the SAR is a clear and concise definition for "remote access". This seems to have been generally interpreted to-date as external access from outside the corporate enterprise environment. However, with CIP-011, NERC seems to be moving towards an interpretation as "any electronic access from outside the ESP". This is a significant change if that is the intent, and could require entities to make major infrastructure and procedural modifications.</p> <p>There has been much discussion over the last several months regarding the permissible use of remote access by entities. It seems NERC has been leaning towards a stance that external, interactive, remote access is permissible (given the proper controls) for administrative or maintenance support. However, this use for remote operations (with full-control capabilities) seems to not be allowed. The SAR as written does not address this point if that is the intended position, and E.ON U.S. believes the intent should be clearly stated.</p> <p>One additional note on the SAR...one of the most ambiguous requirements discussed over the past several months regarding NERC's guidance on remote access stated that the devices utilized to connect remotely must be documented and treated as CCA's. This implies that these devices must also be afforded the physical security protections (i.e., the 6-wall boundary). If this physical security requirement must be met, this effectively negates the ability for any sort of "mobile device", such as a laptop, to be utilized outside a protected security perimeter. Despite</p>

Voter	Entity	Segment	Vote	Comment
				repeated attempts to have this clarified, to-date we have been unable to get an opinion on this specific point from NERC/SERC. Without this exception, the majority of use-cases for our remote access will not be permitted, making all of these additional controls unnecessary.
Mike Laney	Luminant Generation Company LLC	5	Negative	Although Luminant is in support of R6.3.2 and R6.4, we cannot support R6.3 or R6.3.1 as we feel it will reduce the security of the ESP and is in conflict with other requirements. Luminant would propose the following alternative language. R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point to those required to support the remote access: R6.3.1. Provide encrypted communications between the remote node and the intermediate device or system in R6.4.
S N Fernando	Manitoba Hydro	5	Negative	<p>General Comments:</p> <ol style="list-style-type: none"> <li>1. Remote Access: It is unclear whether "remote access" refers to "remote interactive access" of a person to the Cyber Asset, or remote machine-to- machine access with the Cyber Asset. Both these types of access are distinct, and have different security solutions. If the intent is to address the person to Cyber Asset access, and the machine-to-machine Cyber Asset access, then they should be addressed separately in the standard.</li> <li>2. Removal of Technically Feasible: Legacy devices may be unable to meet the prescriptive technical requirements of the proposed R6, and therefore the requirements should only apply where technically feasible, and be subject to the Technical Feasibility Exception process.</li> <li>3. Version History: The standard applies to Cyber Assets, not Critical Assets. The reference to "for support staff maintenance" in the Action is not reflected in the accompanying SAR, which makes vague references to remote access. The proposed standard, as written, could be interpreted to apply to remote access for any purpose.</li> </ol> <p>R6 - The current wording is too broad. Suggest wording "The Responsible Entity shall implement the following controls before granting remote interactive access to its Electronic Security Perimeters, to prevent unauthorized access to its Cyber Assets within its Electronic Security Perimeters."</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.1.1 - Vendor personnel who provide technical support for Cyber Assets within the ESP should also be authorized. Suggest wording "... vendor personnel who have authorized electronic access who provide technical support ...".</p> <p>R6.2.1 - The current wording could be interpreted as requiring multifactor authentication to, and including, the Cyber Asset within the ESP. Not all Cyber Assets within the ESP will support multifactor authentication. Multifactor authentication to the ESP should be sufficient.</p> <p>R6.3 - The actual intent of Requirement 6.3 is unclear. Regarding the statement "Restrict the protocols ... to protocols that: Provide encrypted communications .... " Is the intent that the protocol provide the encryption? Not all protocols provide encryption, although other technologies can encrypt communications, but not at the protocol level. Is the intent that the protocol support the authentication? Not all protocols support authentication, although other technologies can support authentication. The intent of the requirement should be to require secure communications, without being overly prescriptive. The terms "remote node" and "host" are not clear, are not defined, and are not used anywhere else in CIP-003 through CIP-009. R6.3.1 - Requirement 6.3.1 specifies that encrypted communications must terminate at a host within the ESP. VPN tunnels that terminate at a firewall provide the same or a better level of security as VPN tunnels that terminate at an internal proxy server, are a mainstream IT architecture and should not be excluded. This architecture also has the advantage of supporting unencrypted traffic within the ESP, which allows the firewall's anti-malware software and the IDS sensors inside the ESP to analyze the traffic. The current wording excludes this architecture. R6.4 - The wording, the intent, and the security value of Requirement 6.4 is unclear and this requirement should be removed.</p>

Voter	Entity	Segment	Vote	Comment
Steven Grego	MEAG Power	5	Affirmative	As stated by MEAG Power on 9/14/10 during the Pre-Ballot Window for this proposed new standard, MEAG Power has concerns about the meaning of the current language being proposed in R6.3.1. MEAG Power is voting "yes" under the assumption that the goal of an entity providing "encrypted communications between the remote node and the host inside the Electronic Security Perimeter" could be accomplished by an entity providing encryption between the remote node and an intermediate device - so that any external system(s) used for remote access does not communicate directly with a Cyber Asset within the Electronic Security Perimeter.
Don Schmit	Nebraska Public Power District	5	Negative	<p>R6.2.1 Comments:</p> <ul style="list-style-type: none"> <li>Does the RSA authentication system equipment need to be on the inside of the ESP and PSP?</li> <li>Does the system (server/PC) that authenticates the remote user need to be on the inside of the ESP and PSP? For example, could a system (Windows Terminal Server or dedicated PC) on the outside of the ESP and PSP be used as a workstation that validates user authentication via multifactor authentication? The user then launches an application that then allows them to authenticate to a CCA or non-CCA without multifactor authentication but via the ESP controls limit access by IP address and port.</li> </ul> <p>R6.2.2 Comments:</p> <ul style="list-style-type: none"> <li>Is the duration of the interactive session in relationship to the first system or all subsequent systems as well? For example, I log into Non-CCA Server A. Server A is inside the ESP. It prompts me for my multifactor authentication as it is the initial system I access through the ESP. From Server A I start a remote session to CCA Server B which is not directly accessible through the ESP. Do I only need log the duration of access to Server A or do I also need to record separately the access duration to Server B?</li> </ul> <p>R6.3.1 Comments:</p> <ul style="list-style-type: none"> <li>What levels of encryption are acceptable? DES, 3DES, Blowfish, AES?</li> <li>Can a VPN tunnel be utilized between the remote node and a VPN appliance on the ESP or does the encryption have to be between the first internal host and the external host communicating into the</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>ESP?</p> <ul style="list-style-type: none"> <li>If VPN tunnels are allowed, split tunnel configurations should be disallowed.</li> </ul> <p>R6.4 Comments: This seems confusing as all devices within an ESP are either Critical Cyber Assets (CCA) or Non-Critical Cyber Assets (Non-CCA). Is this meant to say "Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a <b>Critical</b> Cyber Asset." or is this to mean that communications are required to go through a control/protection device such as a firewall or inline IDS?</p>
Michael K Wilkerson	Northern Indiana Public Service Co.	5	Negative	<p>General Comments</p> <ol style="list-style-type: none"> <li>1. <b>NIPSCO</b> would like a concise definition of what the scope of remote access is. Is remote access explicit to the source of the communication; Internet, corporate network, or anything outside the ESP? Does remote access include ESP-to-ESP communications? Is remote access explicit to a type of communication; application to application non interactive communication, system to system non interactive communication, or specifically administrative interactive access? In order to ballot on the addition of a remote access requirement, a definition and scope need to be provided for the term remote access.</li> <li>2. NIPSCO recommends that the drafting team consider a longer implementation plan. The changes that may be required would be difficult to implement in the larger, more complex environments in such a short period of time. The drafting team needs to consider the processes required for implementing changes to existing entity environments (e.g. purchasing hardware, change management, documentation updates, testing, potential non-compliance issues as entities implement changes to existing critical environments, etc.), and recognize that it would be extremely difficult to implement in a six to nine month period. NIPSCO recommends extending the implementation plan to 12 – 18 months.</li> <li>3. The modifications to this CIP-005 standard are often related to</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>numerous other CIP standards. NIPSCO recommends striking the entire CIP-005-4 R6.1 and sub-requirements. The section addresses user management and authorization of users who have authorized cyber access to critical cyber assets. NIPSCO feels that this section conflicts with CIP-004 R4 and is unnecessary.</p> <p>4. The drafting team should consider removing the entire CIP-005-4 R6 Remote Access requirements and incorporating some of the key components into the existing CIP sections 2.3 and 2.4. That would entail not removing the current requirements and expanding interactive access to include remote access and it would eliminate the overlap of other CIP standards.</p> <p><b>Requirement-by-requirement issues:</b></p> <p>R6.2 – NIPSCO recommends this section to be clarified to include only interactive logins. The external interactive access language from requirement 2.3 should be added back in this requirement to clarify that remote access should only include interactive access into the ESP. In addition, NIPSCO recommends explicitly excluding non-interactive access (e.g, application-to-application, machine-to-machine) from the CIP-005 Remote Access requirements.</p> <p>R6.2.3 – The drafting team needs to clarify “retain all logs”. If ESP logs are the only required logs to be maintained, this requirement should be removed as CIP-005 R3 addresses the monitoring and logging of ESP access. If the entity were required to capture the entire path of remote access logs it would pose technical challenges, expand the scope of devices to retain logs from beyond the scope of the CIP standards, and depending on current entity technology structure this may require additional resources.</p> <p>R6.3 – Where would the encryption initiate and terminate? The drafting team needs to clarify whether it is the entire path needs to be encrypted or something less (from a VPN concentrator, from the intermediate device suggested in 6.4, to the ESP, etc this complexity will vary by entity, but the intent of the requirement needs to be clearly defined). The current</p>

Voter	Entity	Segment	Vote	Comment
				<p>wording suggests that the encryption would initiate from the desktop and terminate at the host within the ESP. NIPSCO believes this would be a major issue as it may classify hosts in your ESP as access points if they are termination points for remote access.</p> <p>R6.4 – NIPSCO believes this to be inconsistent with R6.3. It would be extremely difficult to do end-to-end encryption and use an intermediate device. The requirement needs to include language to clarify where the encryption must be utilized, or strike the requirement. In addition, the requirement to have an intermediate device as a jumping point, depending on entity implementation may or may not consider the intermediate device as a CCA. This wording will leave open the interpretation of whether the intermediate asset should be a CCA or not. Further clarification regarding what requirements would be applicable? All CIP requirements or a subset – if all then the intermediate device would be a CCA, as a CCA would be in an ESP, however as an intermediate device would need to reside in an ESP different than the native CCA ESP and you would need an intermediate device to talk to the intermediate device and so on. This requirement may go beyond the scope of the current CIP-002 standards in defining cyber assets within the scope of CIP. Further clarification around this requirement is necessary.</p> <p><b>Measures:</b></p> <p>NIPSCO recommends removing the additional measure if the requirements are realigned back under requirements 2.3 and 2.4.</p>
Richard Kinias	Orlando Utilities Commission	5	Negative	<p>R6 is currently very poorly worded and suggest changing the wording to the following to remove ambiguity in using words such as “if” and “wish” and remove the interpretation surrounding the word “remote”:</p> <p>Remote Access Controls – The following controls shall be implemented for all access to Cyber Assets across an ESP boundary:</p> <p>Additionally, Requirement 6.3.1 could be in direct contradiction to requirement 6.4. if encryption between a remote node and a host node is interpreted to be a serial chain of encrypted tunnels as opposed to a single tunnel between the remote node and the host. Requirement 6.3.1 seems</p>

Voter	Entity	Segment	Vote	Comment
				to force an interpretation of a serial chain of tunnels. An additional interpretation could be that both encryptions need to be in place via a VPN from remote host to ESP control point for strong authentication, then an SSL tunnel or some other encryption within the established tunnel would additionally be required (i.e. HTTPS inside a Cisco VPN). Any requirement that may result in an interpretation request must be reworded to remove the ambiguity.
Sandra L. Shaffer	PacifiCorp	5	Negative	<p>Regarding the deletion of CIP-005-3 R2.4, we have no objection.</p> <p>Regarding the additional material of R6, we have the following comments:</p> <p><b>R6</b> -- "Remote Access" is not defined adequately. Does Remote Access refer to "human interactive access" or does it encompass any and all network communications between a host internal to the ESP and a host external to the ESP? Is there any distinction between read only remote access and write enabled remote access? Have we abandoned the distinction between human interactive access and system to system communications?</p> <p><b>Recommendation:</b> Define "Remote Access" such that it is qualified as "human interactive access".</p> <p><b>R6.1</b> -- This language indicates that only two categories of individuals may be granted remote access: employees of the entity and vendor technical support personnel. This would exclude third parties who simply need to retrieve data, but are not employees of the entity nor provide technical support. For example, Cowlitz Public Utility District is a non-operator owner of the Swift No. 2 generating facility operated by PacifiCorp, and thus currently has access privileges to the site and data. Cowlitz PUD also has some access rights to data related to the Swift No. 1 facility which is owned and operated by PacifiCorp. Under the new language in R6.1, Cowlitz PUD, as a third party entity, would lose any remote access privileges, which is problematic.</p> <p><b>Recommendation:</b> Avoid categories of personnel and simply</p>

Voter	Entity	Segment	Vote	Comment
				<p>require that all remote access comply with the principle of "least privilege" or add business partner as an attribute for qualification of remote access.</p> <p><b>R6.3</b> -- This section needs a technical feasibility exception for legacy equipment that does not support encryption. For example, telnet protocol which may well be encrypted by virtue of it's traversing a VPN between the Access Point and the VPN client, but would not be encrypted between the internal host and the Access Point.</p> <p><b>Recommendation:</b> Include the phrase, "where technically feasible".</p> <p><b>R6.4</b> -- This language needs clarification. What is meant by "communicate directly"? Specifically, at what point in the OSI stack are we inserting this "barrier" to direct communication? Layer 3 (firewall - perhaps NAT/PAT)? Layer 4-7 (proxy)?</p> <p><b>Recommendation:</b> Drop this requirement completely.</p>
Gary L Tingley	Portland General Electric Co.	5	Negative	<p>PGE is against the proposed revisions because they will increase uncertainty in two main areas. First, the proposed revisions would lead to increased confusion about whether CIP-005 governs machine-to-machine interactions as well as human-to-machine interactions. CIP-005-3 Requirement 2.4 applied to both machine-initiated and human-initiated access, and by removing this requirement and replacing it with the proposed Requirement 6 it appears that the Standard Drafting Team proposes to limit the scope of this standard to only human-initiated access. In particular, proposed Requirement 6.3.1 seems to be intended to only apply to human-initiated access, as the term "encrypted communications" does not specifically apply to machine-initiated access. The revision needs to make clear what types of access are covered. Second, the proposed wording of R6.4 is not specific enough. It is not clear what specific devices would be included in an "external system used for remote access." This could be read to include the specific computer that the remote user is operating or the remote access system that is allowing such access. In addition, the NERC definition of the term "Cyber Asset" includes any programmable electronic devices and communication networks, which makes it impossible to comply with the requirement as written. PGE</p>

Voter	Entity	Segment	Vote	Comment
				believes that adopting this standard without addressing these potential area of confusion would fail NERC's burden to adopt requirements that define specific obligations.
Tim Hattaway	PowerSouth Energy Cooperative	5	Negative	Remote access connection requirements are not written clearly.
Annette M Bannon	PPL Generation LLC	5	Negative	<p><b>General comments</b></p> <ul style="list-style-type: none"> <li>Define the term 'Remote Access'. Assuming 'remote access' is meant to be interactive remote access, define remotely as specifically as possible.</li> <li>State that 'Remote Access' means interactive access and not machine to machine access. Define as specifically as possible.</li> <li>Remote access should not include ESP to ESP communication within Registered Entities network.</li> <li>Some of the requirements in R6.x as written may not be technically feasible for all assets that are within an ESP that require the capability for remote communication.</li> </ul> <p><b>R2.4</b> Original requirement deleted. No comment.</p> <p><b>R6.1.1</b> The current wording in the proposed standard is covered by other standards. Additionally, this language could imply that vendor personnel do not need to be authorized by the asset owner. This sub-requirement should be removed.</p> <p><b>R6.1.2</b> The current requirement for list of accesses and review are covered by CIP-004 R4.1 and CIP-007 R5.1.3. This requirement is redundant and should be deleted. If this requirement remains, are separate authorized access lists required for remote access?</p> <p><b>R6.1.3</b> This requirement combines two activities together that are very different in nature. Verifying who has been given authorized access and if that access is still valid is covered in CIP-004 R4.1 and CIP-007 R5.1.3. This new</p>

Voter	Entity	Segment	Vote	Comment
				<p>requirement is requesting a verification of the technical implementation to ensure the remote access is secure which would be accomplished by a vulnerability assessment, similar to CIP-007 R8. Suggest this be a sub-requirement of R6.2 which states only authorized individuals can establish remote access to the ESP.</p> <p><b>R6.2</b> Define multi-factor authentication. This was done in a subsequent release of a draft Secure Remote Access document. Ensure this is finalized with the CIP-005 changes.</p> <p><b>R6.2.1</b> Clarify when use of multi-factor authentication is required. Multi-factor authentication is required when crossing the ESP to access a cyber asset. Is multi-factor authentication required when crossing into the Corporate Network?</p> <p><b>R6.2.2</b> Systems may not be capable of accurately, or meaningfully, tracking or providing duration of access, if at all feasible. Consider the need for this logging.</p> <p><b>R6.3.1</b> Clarify what traffic needs to be encrypted. Proposed language says 'encrypted communications between the remote node and the host inside the ESP' and there is no TFE mentioned. Not all 'hosts' inside an ESP are capable of supporting encryption. Can a TFE be taken? Clarify or rephrase to 'Provide encrypted communications between remote access points to the ESP access point, where technically feasible.'</p> <p><b>R6.3.2</b> This requirement is a design requirement which should be a sub-requirement of R6.2.1 if necessary at all depending upon the definition of multi-factor authentication.</p> <p><b>R6.4</b> The requirement as worded is very ambiguous. Is this intended to apply to</p>

Voter	Entity	Segment	Vote	Comment
				<p>remote interactive access by a human or a host-to-host communication?</p> <p>Consider an individual sitting in PSP 1 using multi-factor authentication to access a CCA system in ESP 1 in PSP 1 and the CCA system sends a transaction from ESP 1 to CCA in ESP 2 in PSP 2. Is this remote access as an individual initiated the transaction? Or not, because the system is making the connection, host to host? Would this transaction need to pass through a jump server? Or is R6.4 intended to mean an individual sitting in a remote location using multi-factor authentication to access a CCA system in ESP 1 in PSP 1? More generally, is a jump server required for traffic between all assets?</p>
Wayne Lewis	Progress Energy Carolinas	5	Negative	<p><b>General comments:</b></p> <ul style="list-style-type: none"> <li>• A definition should be included for remote access that emphasizes human-to-machine interaction and excludes machine-to-machine and application access. We believe the emphasis on support and maintenance is key for some entities so that concept should be included in the definition. The drafting team discussed the idea used in the CIP-011 draft...something like “for the purpose of this standard...remote access is...” It was mentioned in some discussions that we do the same for “multifactor” but we believe the addition of “minimum of two-factor” is sufficient.</li> <li>• Understanding the direction to make changes in this one standard and for it to be a standalone set of requirements for secure remote access, the consensus is strongly on the side of removing the requirements that are addressed elsewhere in the CIP standards. With this feedback, we believe we need to assess the approach and decide how to remove overlap and duplicity, e.g. R6.1 Access lists, 6.2.2 monitoring/logging, etc.</li> </ul> <p><b>R6.2.1:</b> We recommend replacing the original text with:  “Require the use of multifactor authentication, with a minimum of two factor authentication, to establish remote access to Cyber Assets within an Electronic Security Perimeter.”</p> <p>Adding “with a minimum of two factor authentication” clarifies what is required.</p>

Voter	Entity	Segment	Vote	Comment
				<p><b>R6.2.2:</b> Replace “time and duration” with “login time and logout time”. This is information that most systems will be able to log.</p> <p>R6.3 has the following problems:</p> <ul style="list-style-type: none"> <li>• R6.3 addresses restricting protocols at access points to the ESP. Restricting protocols at ESP access points is addressed in R2 and does not need to be addressed, and should not be addressed in two different requirements.</li> <li>• R6.3.1 implies that remote access communications must encrypted end-to-end. This is technically challenging, administratively burdensome and not necessary for a secure remote access solution.</li> <li>• R6.3.2 is redundant to R6.1 – it basically states that R6.1 needs to be enforced. That is an unnecessary statement.</li> </ul> <p>To correct these problems, we recommend R6.3 and its sub-requirements are replaced with the following:  “Implement the remote access system such that communications are encrypted whenever they traverse an unprotected network or a public data network.”</p> <p>Note: “Public data network” is defined in Federal Standard 1037C.</p> <p><b>R6.4:</b> As written, this requirement is impossible – the external system must communicate with Cyber Asset. Replace “Cyber Asset” with “Critical Cyber Asset.”</p>
David Murray	PSEG Power LLC	5	Negative	<ol style="list-style-type: none"> <li>1) There is no definition of remote access. There needs to be an agreed to definition. Does it include interactive, human user access? Does it include computer to computer interfaces? What about access to an intermediary that in turn talks to the ESP devices? PSEG suggests that remote access for this requirement be restricted to interactive, human user access through the ESP boundary into the ESP protected network.</li> <li>2) Also needed is a definition of multifactor authentication placed in the standard rather than rely on the supporting guide document.</li> <li>3) In R.6 it should be clarified that access controls and user lists for multiple ESPs can consist of a combined control and list for all ESPs.</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>4) What does "validate the record of individuals with authorized remote access" in R6.1.2 mean? Must entities validate every access attempt or only validate the list of authorized users? Please clarify.</p> <p>5) R6.1.2/6.1.3 should be incorporated as a sub requirement for R6.2 such as: "Review the list of those authorized to remotely access Cyber Assets within an Electronic Security Perimeter at least once each calendar year, with no more than 15 months between reviews and verify that access controls implemented pursuant to Requirement R6.2 only allow access to individuals authorized for that access."</p> <p>6) R6.1.1/R6.1. should be part of R6.1 and eliminate the sub requirements Suggest it be revised to read as follows: "R6.1. Establish, implement, and document procedural controls to authorize remote access to the Electronic Security Perimeter limiting access to those Responsible Entity's personnel who have authorized electronic access to those Cyber Assets and require remote access and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter."</p> <p>7) R6.2.1 should be revised to (1) require multifactor authentication for remote access to the ESP but not to access CCAs inside the ESP since the latter may not be possible to implement, or provide for a TFE and (2) provide for a TFE for logging the duration of access since that is not possible with many systems and devices.</p> <p>8) R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. It should be sufficient for the encryption to terminate at device establishing the Electronic Security Perimeter. Why does the encryption need to go all the way to the device? In some cases it may need to but there should be no general requirement that all communications within an ESP be encrypted. This requirement is too prescriptive and should be clarified to indicate it allows the encryption to end at the access point to the ESP.</p>

Voter	Entity	Segment	Vote	Comment
				9) R6.4. Should provide for a TFE for systems or software that do not support the use or relay or proxy systems that appears to be required as now written.
Thomas J. Bradish	RRI Energy	5	Negative	<ol style="list-style-type: none"> <li>1. NERC needs to explicitly define "remote access" for this standard. We believe that remote access is an individual using a cyber asset outside the Electronic Security Perimeter to login and connect to a Cyber Asset within the Electronic Security Perimeter. We do not believe that remote access is an application server (i.e. such as an EMS server) collecting data from a plant device (example: RTU) within the Electronic Security Perimeter.</li> <li>2. Requirement R6.3.1 needs clarification. More specifically, NERC needs to define "remote node" and to define "host". We believe that the remote node is most likely the "intermediate device" required in R6.4 and the host is a cyber asset within the Electronic Security Perimeter.</li> <li>3. Requirement 6.4 should read: Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset within the Electronic Security Perimeter. Additionally, "external system" should be defined as cyber asset used by an individual to log into and connect to the intermediate device for the purpose of subsequently logging into a cyber asset within the Electronic Security Perimeter.</li> </ol>
Bethany Wright	Sacramento Municipal Utility District	5	Negative	<p>Sacramento Municipal Utility District (SMUD), while supporting the Standard and its related technical architecture set forth in the draft implementation guide, is unable to support a "Yes" vote at this time due to a lack of definition of key elements and procedural ambiguities in the draft Standard.</p> <p>If the Standard remains as drafted, the issues noted above would become problematic realities that Registered Entities must then meet in order to remain compliant. Clarity and a common understanding throughout the industry is essential.</p>

Voter	Entity	Segment	Vote	Comment
				<p>SMUD suggests rewording the current draft of CIP-005-4 to resolve several areas of ambiguity and potential conflict with CIP-004-3. SMUD feels this could be best resolved by referring to the applicable provisions in CIP-004-3 rather than requiring new and different timelines and procedures to be implemented. Taking advantage of processes and disciplines already established by the Registered Entities will further support cyber security and reliable services.</p> <p>Suggested changes include:</p> <ol style="list-style-type: none"> <li>1. Define "remote access"- as "any external communication originating from or through any untrusted telecommunications infrastructure into a registered entity's Electronic Security Perimeter(s) computer network(s)."</li> <li>2. R 6.1.1 is redundant with R2.4.1 and is already covered in part by CIP-004 R4 which requires that anyone including vendors with access be maintained on a list. 6.1.1 seems to differentiate between people on that list ("authorized") versus vendors providing support.</li> <li>3. R6.1.2 requires that the access lists be reviewed "yearly" and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. WECC has identified yearly for compliance purposes as 12 months plus or minus a month. The timelines required in the proposed draft CIP-005-4 R6.1.2 should be consistent with the timelines and expectations outlined elsewhere in the CIP Standards</li> <li>4. R6.1.3 Also seems to be redundant with CIP-004-3 R4. SMUD views the intent of securing remote access is to ensure that we protect the communications across the untrusted communication link and that we ensure authentication, authorization and accounting of the user connecting. Establishing the access point to the ESP as the secure connection is in line with the case studies provided in the guidance document</li> </ol>
Glen Reeves	Salt River	5	Affirmative	SRP requests that clarification of the proposed requirement R6.4 be

Voter	Entity	Segment	Vote	Comment
	Project			provided with examples of acceptable implementations.
Michael J. Haynes	Seattle City Light	5	Negative	While we agree with the majority of the changes recommended by the Standard Drafting Team, we nevertheless voted negative because of Requirement 6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. First, we do not believe this requirement will effectively enhance security. Specifically, by forcing end-to-end encryption for remote communications but not for sessions that originate locally provides little security benefit if you leave internally-sourced sessions in the clear. We are unaware of any other regulatory frameworks that require end-to-end (host-to- host) encryption, including PCI and HIPAA. Normal practice is to terminate encryption at the gateway. Further, this proposal introduces key management issues and could introduce operational issues if encryption fails and connections are not possible. This model introduces more points of failure. Finally, we believe this requirement will be very difficult to accomplish on any widespread basis.
RJames Rocha	Tampa Electric Co.	5	Negative	comments filed
Scott M. Helyer	Tenaska, Inc.	5	Negative	We have several concerns, but primarily we feel that the proposed standard revisions are redundant. Our comments are as follows: R6. Remote Access Controls - If a Responsible Entity wants to grant remote access to its Electronic Security Perimeters, that entity shall implement the following controls before granting such access to prevent unauthorized access to its Cyber Assets: Comment: Covered by existing Standard R6.1. Establish, implement, and document procedural controls that establish an authorization process for remote access to the Electronic Security Perimeter that include the following. Comment: Covered by existing Standard R6.1.1. Limit access to only the Responsible Entity's personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter. Comment: Covered by existing Standard R6.1.2. Maintain a record of all individuals authorized for remote access to Cyber Assets within an Electronic Security Perimeter, and validate the record of individuals with authorized remote access at least once each calendar year, with no more than 15 months between reviews. Comment: Covered by existing Standard R6.1.3. As part of the review of the record of individuals with authorized

Voter	Entity	Segment	Vote	Comment
				<p>remote access (R6.1.2), verify that access controls implemented pursuant to Requirement R6.2 allow access only to individuals included in the record. Comment: How is this verified, achieved, measured, audited? This is redundant, and is asking to document the validity of R6.2.1. The multifactor authentication implies this, or is this requiring biometrics? R6.2. Establish, implement, and document technical controls to ensure that only authorized individuals can establish remote access to the Electronic Security Perimeter. Comment: Covered by existing Standard R6.2.1. Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter. Comment: Covered by existing Standard, multi factor is synonymous with strong authentication. R6.2.2. Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and the time and duration of remote access to Cyber Assets within the Electronic Security Perimeter. Comment: Covered by existing Standard R6.2.3. Retain all logs specified in Requirement R6.2.2 for a minimum of ninety calendar days, or as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008. Comment: Good clarification, document retention was a problem in the previous version. R6.3. Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that: R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. Comment: This would require use of SSL VPN?. Does encryption between the remote gateway and the firewall on the ESP sufficient meet the intent of this requirement, or is encryption required end-to-end? End- to-end encryption would be extremely difficult and prohibitively expensive on some systems R6.3.2. Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1. Comment: Covered by existing Standard R6.4. Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset. Comment: Would SSL VPN meet this requirement, what is the motivation here, is this more hardware? This implies some type of proxy process, which is not typical for most firewalls in use on control networks. It is not clear as to what functionality is allowed or disallowed? Can they provide guidance on this or give examples of what is envisioned here?</p>

Voter	Entity	Segment	Vote	Comment
George T. Ballew	Tennessee Valley Authority	5	Negative	<p>Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this USAR. We fully support the standards development process and all the hard work and commitment by the USAR team members. For this USAR, we have the following concerns which moved us to cast a Negative vote.</p> <p>General Comments:</p> <ol style="list-style-type: none"> <li>1. There isn't a clear definition of the term "remote access." Without this definition there are many ways to interpret this standard. This lack of clarification makes it very difficult to frame questions associated with these proposed new requirements. For example, is communications from a Responsible Entity's non-ESP into their ESP considered remote access? Is communications between a Responsible Entity's ESP's considered remote access, see General Comment #2?</li> </ol> <p>Recommendation: For the purpose of this standard define remote access something like, access originating outside any defined and trusted ESP from a remote location through a data link not controlled by the Responsible Entity, explicitly excluding all Responsible Entity's Inter-ESP communications (e.g. ESP to ESP communications) and non-ESP to ESP communications.</p> <ol style="list-style-type: none"> <li>2. Inter-ESP communications. Without remote access being clearly defined, it isn't clear if Inter-ESP communications is considered remote access. Does this require every ESP to contain an intermediate device or system for remote access? In an environment that has multiple ESP's located on a private network can there be one access point. For example, an organization that has 50 substations that are interconnected on a private network. There is an ESP at each substation with a remote access point being centralized at a control center. Is there an expectation that communication between the control center and the substations, separate ESP's, take place over encrypted communication?</li> </ol> <p>Recommendation: Inter-ESP communications is outside the scope of this requirement. Communications between two defined and trusted</p>

Voter	Entity	Segment	Vote	Comment
				<p>ESP's isn't considered Remote Access. This would imply there is a "mutual trust" between ESP's owned and managed by the Responsible Entity.</p> <p>Specific Comments:</p> <ol style="list-style-type: none"> <li>6.1 - This requirement focuses on account management which is already addressed in other standards. Recommendation: To ensure consistency across the standards we recommend that the same verbiage in CIP-007 R5 is used in this section.</li> <li>6.3.1 - The way this requirements is worded makes it sound like encrypted communications must be used between the remote node and each individual device it is communicating with within the ESP. This isn't technically feasible. Recommendation: Reword the requirement to make it clear that encryption is only required between the remote node (end-user device (e.g. laptop)) and the gateway into the ESP (e.g. VPN Access Point).</li> <li>6.3.1 - It is unclear if language reference to "the host" means the cyber asset within the ESP versus an intermediate device or system as described in 6.4. Recommendation: Reword 6.3.1 and 6.4 to provide more clarity.</li> </ol>
Karl Bryan	U.S. Army Corps of Engineers Northwestern Division	5	Negative	<p>To put this into perspective all remote access isn't into a computer center, which these rules seemed geared towards. Our plants are up to 1200 miles apart - in the future we may be protecting/accessing one asset (switch yard PLC), in that case it's entirely feasible with the wording of R6.4 that you would have more assets involved in the protection of said critical asset than you have critical assets.</p> <p>R6.3.1 - Provide encrypted communications between the remote node and the host inside the ESP. This may not be possible if the host is a PLC or an RTU - there is no encrypted protocol that can be used to communicate directly to the PLC.</p> <p>R6.4 - using an intermediate device to communicate to a PLC or RTU may not be possible</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.4 also seems to be in direct conflict with R6.3.1 6.4 states that an intermediate device so that remote access does not communicate directly with a cyber asset. 6.3.1 seems to allow communication directly to the host as long as it's encrypted.</p>
Martin Bauer P.E.	U.S. Bureau of Reclamation	5	Negative	<p>The SDT has changed the Standard CIP-005 to address Remote access issues. The changes require specific processes for ensuring that only those who should have access can access and that there is a record of those individuals. The standard language proposed also requires that technical controls are implemented for remote access. The section dealing with this requirement is not clear on what a "technical control" is or what is appropriate for multifactor authentication. These details were expected to be clarified in the measures. The proposed changes require that the remote access device or system does not communicated directly with a Cyber Asset. This does not limit the applicability to critical cyber assets. In addition the following specifics are noted.</p> <ol style="list-style-type: none"> <li>1. The changes do not improve the clarity of the requirements, they only add additional overhead. Until the clarity of the Standard is improved (as an example we would cite the recently published "Secure Remote Access Draft", Sept., 2010) we would not endorse changes to the existing Standard.</li> <li>2. Key terms (e.g., multifactor) and conditions (remote access from sites on the Internet verses those within the same routed network) have not been clearly defined nor have they been differentiated from a realistic requirements standpoint.</li> <li>3. Some of the requirements (boundary analysis of inbound/outpoint traffic) is inherently defeated as a result of the requirement to encrypt communications at the internal (host) node.</li> </ol> <p>In addition:</p> <ul style="list-style-type: none"> <li>• R2.2 - Change to read "Entity shall enable only logical ports and services..."</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> <li>• R2.4.4 - Change to read "The controls used to secure dial-up accessible connections, where they are permitted"</li> <li>• R3 - Change to read "document an electronic or manual process(es) for monitoring and logging remote access..."</li> <li>• R4.2 - Change to read "verify that only logical ports and services..."</li> <li>• R5.1 - Change to read "shall ensure that all documentation required by Standard CIP-005-4 reflects the operational configuration and processes within no more than 90 days of any change..."</li> <li>• R5.3 - Change to read "shall retain electronic access logs for ESP access points for at least..."</li> <li>• R5.3 - Change to read "Logs related to reportable incidents associated with ESP access points shall be..."</li> <li>• R6.1.1 - Change to read "Limit access to only personnel or technical support vendors who have authorized electronic access to Cyber Assets within the specific ESP."</li> <li>• R6.2.1 - See note 2, above.</li> <li>• R6.3.1 - See note 3, above.</li> <li>• R6.4 - This solution is not necessary if some authentication solutions are deployed (e.g., a Radius Server).</li> </ul> <p>Further, such a solution requires additional hardware which, in some situations may add additional resources at sites where a single or few devices are deployed. Suggest this requirement be reconsidered in instances where remote access is not from the Internet (see note 2, above)</p> <ul style="list-style-type: none"> <li>• Suggest the addition of a new requirement, R6.5, reading "ESP to ESP communications, within the same routed network, are not considered remote access."</li> </ul>

Voter	Entity	Segment	Vote	Comment
Bohdan M Dackow	US Power Generating Company	5	Negative	Revision does not clearly define what constitutes "Remote Access", needs to be a defined term. Standard needs to clearly define requirements for each of the different types of remote access - interactive, non-interactive, internet, intranet, etc.
Linda Horn	Wisconsin Electric Power Co.	5	Negative	<p>The proposed standard revision contains many requirements for security specific to certain types of connections and uses, but is lacking clarity on defining those situations and where each specific requirement applies. In order to provide the sufficient guidance, the revised standard should include specific use cases to describe the requirements for, at a minimum:</p> <ol style="list-style-type: none"> <li>1. Accessing a Critical Cyber Asset interactively "Locally." (e.g. directly at the device)</li> <li>2. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, but within the corporate enterprise network.</li> <li>3. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset, and outside of the corporate enterprise network.</li> <li>4. Accessing a Critical Cyber Asset interactively from a different ESP.</li> <li>5. Accessing a Critical Cyber Asset interactively from outside the ESP that contains the Critical Cyber Asset in a disaster recovery scenario or disaster recovery test.</li> <li>6. Accessing a Critical Cyber Asset using a computer, or programmatically from within an ESP.</li> <li>7. Accessing a Critical Cyber Asset using a computer, or programmatically from outside the ESP that contains the Critical Cyber Asset.</li> </ol> <p>The industry would be aided by the provision of theoretical network diagrams within the guidance to depict the interactive access options.</p> <p>For requirement 6, definitions should be developed for:</p> <ul style="list-style-type: none"> <li>• Remote external, interactive access, and</li> <li>• Multifactor authentication</li> </ul> <p>Ideally the resulting definitions should be integrated closely with the use case guidance requested above.</p> <p>The following suggested wordings are provided for requirements 6 through</p>

Voter	Entity	Segment	Vote	Comment
				<p>6.4 to provide clarity and actionable direction:</p> <p><b>R6.1.</b> Establish, implement, and document procedural controls that establish an authorization process for remote external, interactive access to the Electronic Security Perimeter that include the following.</p> <p><b>R6.1.1.</b> Limit access to only the Responsible Entity's personnel who have authorized electronic access to Cyber Assets within the specific Electronic Security Perimeter and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter.</p> <p><b>R6.1.2.</b> Maintain a record of all individuals authorized for remote access to Cyber Assets within an Electronic Security Perimeter, and validate the record of individuals with authorized remote access at least once each calendar year, with no more than 15 months between reviews.</p> <p><b>R6.1.3.</b> As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls implemented pursuant to Requirement R6.2 allow access only to individuals included in the record.</p> <p><b>R6.2.</b> Establish, implement, and document technical controls to ensure that only authorized individuals can establish remote interactive access to the Electronic Security Perimeter.</p> <p><b>R6.2.1.</b> Require the use of multifactor authentication to establish remote interactive access to Cyber Assets within an Electronic Security Perimeter.</p> <p><b>R6.2.2.</b> Implement and document one or more electronic or manual processes for monitoring and logging the user identification, and where technically feasible, log the time and duration of remote access to Cyber Assets within the Electronic Security Perimeter.</p> <p><b>R6.2.3.</b> Retain all logs specified in Requirement R6.2.2 for a</p>

Voter	Entity	Segment	Vote	Comment
				<p>minimum of ninety calendar days, or as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008.</p> <p><b>R6.3.</b> Restrict the protocols allowed to pass through an Electronic Security Perimeter access point for the purpose of remote access to protocols that:</p> <p><b>R6.3.1.</b> Provide encrypted communications between the remote node and the Electronic Security Perimeter.</p> <p><b>R6.3.2.</b> Support authentication controls sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1.</p> <p><b>R6.4.</b> Where technically feasible , Implement an intermediate device or system such that the external system used for remote interactive access does not communicate directly with a Cyber Asset.</p>
Edward P. Cox	AEP Marketing	6	Negative	<p>AEP recommends a longer Implementation Plan. Getting this implemented in a complex, multi-ESP environment while preserving reliability is a significant effort. Purchasing and implementing hardware quickly, while following procedures for change management is simply not possible in a six to nine month period and AEP feels that 12 to 18 months might be more appropriate. AEP is requesting clarity on what constitutes "remote access"? There are at least three scenarios for where the traffic originates: 1) internet, 2) corporate network, 3) another ESP. Which one(s) constitute remote access? AEP would assert that at least #3 is not "remote access" and quite possibly not #2 as well. As such, the drafting team should consider explicitly excluding hosts within a separate ESP from the remote access standard. Further, machine-to-machine ("non-interactive") access may need to be excluded from remote access, even if it involves a machine outside of the ESP. In addition, the change to CIP-005 appears to introduce unnecessary overlap with other standards and requirements.</p>

Voter	Entity	Segment	Vote	Comment
				<p>Below are some specific comments in the requirements of CIP-005.</p> <p>R6.1 - This text doesn't belong in CIP-005 as it is a user management issue. This requirement belongs, more properly, in CIP-004, R4. It appears to overlap, and perhaps conflict with CIP-004, R4. If you're compliant with CIP-004, R4 presumably you should be able to demonstrate compliance with CIP-005, R6.1. Demonstrating compliance twice seems unnecessary and cumbersome.</p> <p>R6.2 - There are significant technical issues around duration of access, and yet there is little reliability value. Proving you have the duration of access for each user access appears to be enormously time consuming and resource intensive. If there is no reliability value to tracking duration of access (and it appears there is not), we suggest that it be removed from the requirement. If it remains in the requirement, Responsible Entities will have to demonstrate compliance - and RE auditors will have to measure it.</p> <p>R6.3 - When and where exactly would encryption be required? Which remote access scenarios would require encryption? Is encryption to the intermediate device in R6.4 sufficient? What is the purpose of the "encryption"? Is it to preserve the confidentiality of the data? If so, why? Is it to provide data integrity? AEP would recommend striking the requirement for encryption. It's very difficult to demonstrate compliance, and appears to add little reliability value.</p> <p>R6.4 - At a minimum, recommend broadening the definition of intermediate device to include the Electronic Security Perimeter Access Point itself. There are many different ways to implement this security control, and as written, this requirement seems to expect a very specific technical solution. Further, for multiple ESPs, a single intermediate device should be sufficient - assuming it's within an equivalent ESP. As discussed above, ESP-to-ESP traffic should be explicitly excluded from "remote access."</p>
Brenda S. Anderson	Bonneville Power Administration	6	Negative	<p>Unanimous consensus of reviewers is a 'no' vote to these changes. All felt that the proposed changes do not contribute substantively to the current version. The previous version was sufficient. Reviewers also objected to being directed on "how" to comply as opposed to "what" to be complied with. Reviewers also agreed that this draft needs a better definition of</p>

Voter	Entity	Segment	Vote	Comment
				<p>“Remote Access.” For example, is it access from location external to ESP? Or, is it access from outside controlled networks but within the Responsible Entity’s system? Or, is it access from a location that external to the Responsible Entity’s systems altogether?</p> <p>Other than the new definition of “Annual” nothing was found to be agreeable within the proposed changes.</p> <p>Comments and Recommendations are listed below.</p> <p>The existing CIP-005-3 R2.4 makes is clear that strong procedural and technical controls must be implemented to ensure “authenticity” of the access party. In some cases, that could mean encryption. It would be helpful to have a Security Guideline for CIP-005 that gave examples of strong technical and procedural controls.</p> <p>A definition of “remote access” needs to be established.</p> <p>R6 states “...implement the following controls before granting access.” It would be best to implement technical and procedural controls once to support remote access and handle granting access authorizations separately.</p> <p>R6 may conflict with the current CIP-005 R3.1 which includes the verbiage “where technically feasible.” Since TFE’s are not allowed in the future, shouldn’t the “where technically feasible” language be deleted? The new R6 should apply to dial-up.</p> <p>R6.1 is redundant with R2.4.1 (currently R2.5.1). We understand that CIP-005-3 R2.4 and R2.5 pertain only to external user interactive access (remote user access) thru the ESP for access to one or more Cyber Assets. Access to ESP ACMs (access control and monitoring) cyber assets is address by CIP-005 R1.5. If a new CIP-005 R6 requirement to address remote access is added, then the current CIP-005-3 R2.4 and R2.5 should be deleted and included in the new R6.</p> <p>R6.1.2 and R6.1.3 are redundant and conflict with the current CIP-005</p>

Voter	Entity	Segment	Vote	Comment
				<p>R2.5.3.</p> <p>R6.2.2 and R6.2.3 are somewhat redundant with the current CIP-005 RCIP-005 R3.2.</p> <p>R6.4.The intermediate device or system for remote access should not be an external system.</p> <p>A suggested rewording</p> <p>R6. Remote Access Controls - To prevent unauthorized access to its Cyber Assets, where interactive access into the Electronic Security Perimeter is to be enabled, prior to granting such access the Responsible entity shall:</p> <p style="padding-left: 40px;">R6.1. Implement and document procedural and technical controls to ensure that such access is controlled and limited to authorized personnel.</p> <p style="padding-left: 40px;">R6.2. Restrict remote access to Electronic Security Perimeter access points to methods which support authentication controls sufficient to verify the identify and authenticity of individuals remotely accessing Cyber Assets within the Electronic Security Perimeter.</p> <p style="padding-left: 40px;">R6.3. Provide logging of all successful and failed access attempts.</p>
Robert Hirschak	Cleco Power LLC	6	Affirmative	None
Nickesha P Carrol	Consolidated Edison Co. of New York	6	Negative	<p><b><u>CIP-005-4 Comments</u></b> - Consolidated Edison supports NPCC's comments.</p> <ul style="list-style-type: none"> <li>• An implementation plan has not been posted.</li> <li>• The SAR is too broad in its scope. The SAR should be more specific on the type of Remote Access covered.</li> <li>• Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)". <ul style="list-style-type: none"> <li>• The updates to CIP-005 do not respond to the SAR's intent of end point protection. The updates only address access across</li> </ul> </li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>the Electronic Security Perimeter (ESP)</p> <ul style="list-style-type: none"> <li>• The current R6 repeats many requirements already specified in R2. The contents of R6 should be moved as a sub-requirement of R2, R2.3 being the corresponding stricken requirement. As posted, some sub-requirements of R6 result in a double jeopardy.</li> <li>• The term "remote access" used in R6 needs clarification. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP"</li> <li>• The language for R6 requires clarification to more accurately reflect the intended scope, specifically as follows: <ul style="list-style-type: none"> <li>•Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</li> <li>•CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</li> <li>•It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer.</li> </ul> </li> <li>• Requirement R6.1 should be removed: it duplicates CIP-004 Requirements, resulting in double jeopardy.</li> <li>• Requirement R6.2 should be removed: it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2.</li> <li>• There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural (i.e. a multifactor authentication scheme can be implemented by any mix of technical and procedural controls). By putting this under technical requirements this requirement</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>implies that only technical solutions are acceptable.</p> <ul style="list-style-type: none"> <li>Requirement R6.3 duplicates the ports and services requirements in CIP-005 R4.2: it should be removed.</li> <li>Requiring encryption across the ESP in requirement R6.3.1 to the end-device inside the ESP is against the best practice implemented by many entities of decrypting at or immediately prior to the access point. Encrypting beyond the access point removes the visibility required for content inspection as risk mitigation control.</li> <li>Requirement R6.4 prescribes a specific mitigation control, telling how to implement. The Requirement should be redrafted to specify the control objective and allow entities to implement the specific controls required to achieve the control objective.</li> </ul>
Brenda Powell	Constellation Energy Commodities Group	6	Negative	<p>NERC should revise the proposed standards to clarify the remote access requirements do not apply to communication between Electronic Security Perimeters (ESP). Imposing the proposed remote access controls to communications in between ESPs would reduce effectiveness of existing security controls, assuming that remote access between ESPs could be installed. Additionally, system reliability could be affected if remote access between ESPs reduces availability of CCAs. R6.1.3: Since 6.1.2 establishes the record of individuals with authorized remote access and is referenced, the concluding phrase is unnecessary. Proposed edit: R6.1.3 As part of the review of the record of individuals with authorized remote access (R6.1.2), verify that access controls are implemented pursuant to Requirement R6.2. R6.2.2: Please clarify that the trigger of user logging occurs at the ESP level. Proposed edit: R6.2.2 Implement and document one or more electronic or manual processes for monitoring and logging user identification, and the time and duration of remote access through the Electronic Security Perimeter. R6.3: This requirement is repetitive and unnecessary. R3 and R6.1 already cover the requirements in R6.3. R6.4: Please clarify the intent of this requirement. It does not seem feasible to prevent direct communication with a Cyber Asset. Proposed edit: R6.4 Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Critical Cyber Asset.</p>

Voter	Entity	Segment	Vote	Comment
Louis S Slade	Dominion Resources, Inc.	6	Negative	<p>Dominion believes properly authorized personnel must be allowed to provide remote operational and maintenance support for cyber assets within an Electronic Security Perimeter to maintain reliable operation of the Bulk Electric System. The application of remote access security measures should be carefully applied to avoid inadvertent, adverse reliability impacts. Several specific issues with proposed CIP-005-4 R6 changes must be addressed before the new requirement can be properly interpreted and consistently implemented throughout the industry.</p> <p>R6.1 – This requirement duplicates access control requirements addressed in CIP-005 R2 and CIP-004 R4. Dominion suggests moving requirement R6.1.1 to requirement R2 as a sub-requirement to R2.1. Requirement R6.1.2 repeats and may even contradict access authorization requirements in CIP-004 R4 regarding the review and validation of personnel with authorized cyber access to Critical Cyber Assets (e.g., quarterly access reviews vs 15 months for ESP access). Dominion suggests referring to requirement CIP-004 R4 or CIP-005 R2 (which refers to CIP-004 R4) instead of specifying separate review requirements in R6.1.2 and R6.1.3. If the requirement to validate who has remote access to an ESP once a calendar year is kept, please define a calendar year and clarify how a review is conducted ‘at least once each calendar year, with no more than 15 months between reviews’.</p> <p>R6.2.1 – The deletion of existing requirement R2.3 removes the reference to ‘external interactive access into the Electronic Security Perimeter’. However, the reference to multifactor authentication in this requirement suggests the term ‘remote access’ refers to interactive user access. Do the remote access requirements apply to remote devices that poll devices inside an ESP or data connections between multiple ESPs? The term ‘remote access’ should be more clearly defined.</p> <p>Based on FERC Order 706 paragraph 511, the reference to multifactor authentication is too prescriptive. That Order cited two-factor authentication and digital certificates as <i>examples</i> of strong authentication but did not specify that they were the only methods allowed.</p> <p>R6.2.2 – Dominion questions the feasibility of monitoring and logging the <i>duration</i> of remote access sessions. If this requirement remains, a Technical Feasibility Exception (TFE) should be allowed. Monitoring and logging requirements are already addressed in requirements R3 and R5 of CIP-005 and should be removed from R6.2.2 and R6.2.3.</p>

Voter	Entity	Segment	Vote	Comment
				<p>R6.3 – Serial connections via dial-up modems cannot support protocol/port restrictions or encrypted communications. Dial-up access is addressed in CIP-005 R2. Does CIP-005 R6 apply to dial-up access?</p> <p>R6.3.1 – According to the Purpose statement in the Introduction section of proposed standard CIP-005-4, the standard focuses on the identification and protection of the Electronic Security Perimeter (ESP) and perimeter access points. However, requirement R6.3.1 specifies encryption between a remote node and devices inside the ESP instead of between a remote node and an access point. This practice would prohibit adequate inspection at the access point to insure access has been authorized. The requirement only recognizes end-to-end encryption and does not permit the use of network level encryption.</p> <p>Encryption from a remote access point to a host inside the ESP may not be technically feasible for all device types and precludes intrusion inspection of the traffic through the access point. If this requirement stands a Technical Feasibility Exception (TFE) should be allowed.</p> <p>R6.4 - The requirement to ‘implement an intermediate device or system’ to communicate remotely with a cyber asset within an ESP appears to contradict requirement R6.3.1, which suggests that the remote node must communicate directly with the host using encrypted communications. (In addition, isn’t the intermediate device itself a remote node?) Please define ‘intermediate device or system’.</p> <p>In general, Dominion supports the following measures for remotely accessing cyber assets within an ESP:</p> <ul style="list-style-type: none"> <li>• Multifactor authentication for interactive access.</li> <li>• Introduction of an intermediate device or system so interactive access from an external device does not communicate directly with a cyber asset within an ESP.</li> <li>• Use of encryption from a remote device to an ESP access point</li> </ul> <p>Requiring that 1) anyone granted remote access to an ESP has access to protected devices inside the ESP, and 2) removal of access to all devices inside an ESP requires removal of remote access to the ESP.</p>

Voter	Entity	Segment	Vote	Comment
Mark S Travaglianti	FirstEnergy Solutions	6	Negative	FE believes clarifications are required for the proposed standard and therefore casts a Negative vote with the following suggestions: R6.2.3 - We recommend the deletion of R6.2.3 as data retention is already covered in R5.3. Also, we do not agree that retention of information for investigations should be mandated in a reliability requirement. The retention of information for an investigation is applicable to any standard requirements as specified by the Regional Entity conducting the investigation. This is further reinforced in section 1.3.1 of the Data Retention section of the standard. R6.3.1 - We suggest rewording the requirement to "Provide encrypted communications between the remote node and the Electronic Security Perimeter access control device." We suggest this change because there is no encryption of data traffic "inside" the ESP. R6.3.2 - Requirements R6.3.2 and R6.2.1 appear duplicative. Therefore we suggest deleting R6.3.2 and rewording R6.2.1 as follows: "Require the use of multifactor authentication to establish remote access to Cyber Assets within an Electronic Security Perimeter that are sufficient to verify that the individual remotely accessing Cyber Assets in the Electronic Security Perimeter meets the requirements of R6.1."
Richard L. Montgomery	Florida Municipal Power Agency	6	Negative	The revisions to CIP-005 are ambiguous and open to interpretation. For instance, what does "remote access" mean? Is "view only" remote access? There are often multiple ESPs, is communication between ESPs remote access? R6.3.1 may require that communications to every remote device requires encryption which is not supported on many devices, will this spawn a new round of TFEs?. What does "multi-factor authentication" mean in R6.2.1? What does "intermediate device or system" mean in R6.4? There are too many ambiguities and the standard is far too open to interpretation. Also, care must be taken to not be too proscriptive in singling out one method of providing security while possibly eliminating other, possibly more effective, means of security.

Voter	Entity	Segment	Vote	Comment
Thomas E Washburn	Florida Municipal Power Pool	6	Negative	<p>We question the need for this Urgent Action SAR. The existing standard calls for strong authentication for interactive access at all access points into the ESP. As currently worded, this includes any type of remote access that this SAR is attempting to address. We believe that this SAR and the proposed changes to CIP006 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511. 511. The Commission adopts the CIP NOPR's proposal to direct the ERO to identify examples of specific verification technologies that would satisfy Requirement R2.4, while also allowing compliance pursuant to other technically equivalent measures or technologies. In response to commenters, in discussing digital certificates and two-factor authentication, the Commission was providing examples of strong authentication, not limiting authentication to those options. The Commission is not prescribing the specific methods as an exclusive solution pursuant to Requirement R2.4. The ERO can propose an alternative solution that it believes is equally effective and efficient. If the ERO believes it would be helpful to responsible entities, additional guidance beyond the examples that are eventually included in Requirement R2 can be given in a separate reference document. Since we are directing the ERO to provide guidance on what constitutes strong authentication, it is not necessary for the Commission to respond to ISO-NE's request that digital certifications or two-factor authentication are acceptable methods of authentication. In identifying examples or categories of specific verification technologies that would satisfy Requirement R2.4, the ERO should take into account the specific comments raised in this proceeding. Similarly, while encryption is one method to accomplish two-factor authentication, and is an effective process for ensuring authenticity of the accessing party, for some facilities, we leave it to the ERO in the Reliability Standards development process to evaluate whether and how to address the use of encryption. In the alternative, the ERO may identify verification technologies or categories of verification technologies in a reference document. FERC directed only that NERC provide additional guidance, beyond that provided in the version 1 standard and frequently asked questions, as to what constitutes "strong authentication". This could be accomplished through a guidance document, rather than a change to the standards. In order 706, FERC also clarified that its intent was not to be prescriptive, but to provide examples, and not limit authentication to specific options, which this SAR and the proposed changes to the standard</p>

Voter	Entity	Segment	Vote	Comment
				<p>would effectively do. It appears that NERC intends to restrict or curtail the practice of remotely accessing critical cyber assets within an ESP. While we agree that remote access should be secure, we believe that the ability for operational support personnel and vendors to remotely access these assets is critical to the ongoing reliable operation of the Bulk Electric System. Careful consideration must be given to avoid inadvertent adverse reliability impact through the restriction or curtailment of remote access. Beyond this issue, there are several specific problems with the proposed changes that must be addressed for this standard to be properly interpreted and consistently implemented across the industry. These include: R6 Definition of remote access. It is not clear from the SAR or the standard what is included under the definition of remote access. The SAR uses the terms "access", "secure remote access" and "external access" interchangeably. The standard only uses the term remote access, but it is not clear if that is limited to interactive access on the part of a human being, or also applies to automated access between applications or monitoring functions. For example, a log consolidation tool may connect to devices across multiple ESPs to collect log information. Vendors have read only monitoring tools which poll cyber assets connected to generating units for operational performance and and eventual tuning. It is also not clear if access between trusted ESPs over secure persistent VPN tunnels would be considered remote access. We suggest using the term "remote interactive access", with a definition of such that limits the scope of this requirement to "interactive access on the part of a human being into a NERC designated and protected ESP from a non-NERC protected network outside of that ESP such as the Internet, corporate business network, or a business partner network." R6.2.1 Requirement for multi-factor authentication. The term multi-factor authentication needs to be defined. We are interpreting that this is referring to what is commonly known as two-factor authentication. This is particularly alarming in that it prescribes a particular type of technology which entities must implement which FERC had warned against. Entities should have the option to choose what technology best meets the need in a given situation and NERC should provide examples or guidance on technologies that represent strong authentication. Entities should be allowed to implement authentication technology that is equivalent or better than multi-factor authentication from a reliability perspective that may vary from situation to situation. Additionally, in some of the examples provided</p>

Voter	Entity	Segment	Vote	Comment
				<p>above, applications are not capable of implementing this type of authentication. For ESP to ESP access across a persistent VPN tunnel, this should not even be necessary, as access originates from one secure ESP to another, and traffic is encrypted in transit. R6.2.2 Duration of remote access. Consideration should be given to the feasibility of tracking the duration of access. Not all systems will provide this functionality. R6.3.1 Encryption to the host. This requirement is not technically feasible for most equipment operating in a control system environment today including RTUs, Process Controllers, PLCs,. This equipment generally will not support encryption to the "host" level. In addition, issues such as latency and performance will need to be considered within control systems networks. Encryption of communication inside the access point may also obviate network-level intrusion detection controls that many entities have implemented. As it relates to requirement R6.4 it would appear that the "intermediate device" would be the only "remote node" allowed to access "hosts" within the Electronic Security Perimeter. Additionally, rather than use the term "host" (which we believe is new to the standards) the existing term "cyber asset" should be used. R6.4 Intermediate devices. It is not clear what the intent of this requirement is, and how it would be implemented. We assume that this is referring to a terminal services type of connection for interactive access, however that would not be feasible or necessary for application to application access or access from within another trusted ESP, or the corporate network. Also, the intermediate device itself would be considered a cyber asset used in the control or monitoring of the ESP, so the external system would still be directly connecting to a cyber asset. We would recommend rewording this to state "Implement an intermediate device or system (i.e. terminal server or other similar device) such that the external system used for remote interactive access does not communicate directly through the ESP." Additionally, this seems to conflict with requirement R6.3.1 which assumes that the remote node is communicating directly with the "host" (cyber asset) within the perimeter. R6.1Access Lists - This requirement and associated sub-requirements appear to be redundant to the requirements of CIP004 R4. The CIP004 requirement already calls for a review of lists of personnel with authorized cyber or physical access to cyber assets quarterly. In our opi</p>
Silvia P Mitchell	Florida Power & Light Co.	6	Negative	o R6 Definition of remote access - It is not clear from the SAR or the standard what is included under the definition of remote access. The SAR

Voter	Entity	Segment	Vote	Comment
				<p>uses the terms "access", "secure remote access" and "external access" interchangeably. The standard only uses the term remote access, but it is not clear if that is limited to interactive access on the part of a human being, or if it also applies to automated access between applications or monitoring functions. There are at least three different interpretations of remote access:</p> <ol style="list-style-type: none"> <li>1. Interactive Remote Access (user can make an operational or configuration change),</li> <li>2. Monitoring Remote Access (view only),</li> <li>3. Application/System to Application/System communications over defined ports, services, and protocols (SCADA system controlling a device or exchanging data with another electronic security perimeter or at a non-Critical Asset) and (Electronic Security Perimeter) ESP to ESP)). It is suggested using the term "remote interactive access", with a definition of such that limits the scope of this requirement to "interactive access on the part of a human being into a NERC designated and protected ESP from a non-NERC protected network outside of that ESP such as the Internet, corporate business network, or a business partner network that has the access rights to make an operational or configuration change." The definition should exclude inter-ESP communication within a responsible entity.</li> </ol> <p>o Requirement R6.1, Procedural Controls should be clarified in each of the three subsections (6.1.1, 6.1.2, 6.1.3) to eliminate ambiguity in the requirements, in particular, as to whether the language requires separate access controls and user lists for each ESP or whether all ESP(s) of an operating entity can be combined. NextEra opposes the separation of ESP access into individual ESP access lists.</p> <p>o R6.1Access Lists - This requirement and associated sub-requirements appear to be redundant to the requirements of CIP004 R4. The CIP004 requirement already calls for a review of lists of personnel with authorized cyber or physical access to cyber assets quarterly. In our opinion, authorized cyber access would include remote access; therefore the</p>

Voter	Entity	Segment	Vote	Comment
				<p>individuals with remote access would already be included on the list under CIP004 and would already be reviewed on a quarterly basis. If further requirements around personnel and access lists are needed for remote access, they would more appropriately be addressed by changes to CIP004 R4, which already has a more stringent review requirement than proposed.</p> <p>o R6.2.1 Requirement for multi-factor authentication - The term multi-factor authentication needs to be defined. NextEra interpretation of this is to mean the use of two or more factors (something you know, something you have, something you are) used for authentication.</p> <p>o R6.2.2 Duration of remote access - It does not provide incremental security or reliability and not operationally feasible to implement in most cases. Access times into each security perimeter must be individually logged which would require greatly expanded firewalls and making firewalls a potential failure point for communication impacting the overall goal of improving reliability. If investigation is required the entity could use forensic analysis to identify this information.</p> <p>o R 6.2.2 Monitoring and Logging - This requirement is redundant to the requirement and sub-requirements of CIP005 R3. CIP005 already requires the monitoring of access to the ESP at all access points, and calls for alerting which is over and above what is proposed by the updated standard.</p> <p>o R6.2.3 Log retention - This requirement is redundant to the sub-requirement CIP005 R5.3. This sub-requirement already calls for the 90 day retention of logs.</p> <p>o R6.3.1 Encryption to the host - This requirement is not technically feasible for most equipment operating in a control system environment today including Remote Terminal Units (RTUs), and Programmable Logic Controllers, (PLCs). This equipment generally will not support encryption to the "host" level. In addition, issues such as latency and performance will need to be considered within control systems networks. Encryption of communication inside the access point may also obviate network-level intrusion detection controls that many entities have implemented.</p>

Voter	Entity	Segment	Vote	Comment
				<p>o R6.4 Intermediate devices - It is not clear what the intent of this requirement is, and how to implement it. The presumption is that the requirement is referring to a thin-client terminal server computing solution for interactive access; however, that would not be feasible or necessary for cyber access and communication from one application to another application or access from within another trusted ESP, or the corporate network. Also, the intermediate device itself would be considered a cyber asset used in the control or monitoring of the ESP, so the external system would still be directly connecting to a cyber asset. We would recommend rewording this to state "Implement an intermediate device or system (i.e. terminal server or other similar device) such that the external system used for remote interactive access does not communicate directly through the ESP." It should be clearly defined if an intermediate device or system is a Critical Cyber Asset, a Cyber Asset within an Electronic Security Perimeter, a Cyber asset not required to be within an Electronic Security Perimeter, or an Electronic Security Perimeter Access Point. If not specified, this will lead to multiple different interpretations by different auditors. Additionally, this seems to conflict with requirement R6.3.1 which assumes that the remote node is communicating directly with the "host" (cyber asset) within the perimeter.</p> <p>o Technical Feasibility - Since much of the equipment in place today may not support either encryption or multi-factor authentication, the proposed requirements should provide provisions for filing a technical feasibility exception.</p> <p>o From a related administrative perspective, as a general practice NERC should consider the administrative impact to the industry of re-numbering requirements. In this case, requirement 2.4 is obsolete, and requirements 2.5 and above are being renumbered. While from an aesthetic point of view this might be preferable, NERC should consider the impact to the industry of this seemingly minor change. Any and all documentation and evidence related to compliance with the old requirement will need to be maintained for audit compliance purposes. Current documentation and evidence related to requirements 2.5 and above will all need to be renumbered. The ongoing tracking and maintenance of this documentation</p>

Voter	Entity	Segment	Vote	Comment
				<p>becomes problematic as the historical compliance evidence for a given requirement will not easily align with the current compliance evidence. In some cases this could have even further impacts (TFEs, compliance self certification forms, violations, etc). While this might appear trivial, it creates confusion and unnecessary administrative burden on the part of responsible entities. In cases like this NERC should consider simply delete the words and insert "reserved for future use" and not replace or renumber other affected requirements. The Secure Remote Access Guidance Document addresses some of the concerns identified in the comments listed above.</p>
Paul Shipps	Lakeland Electric	6	Negative	<p>As currently worded, this includes any type of remote access that this SAR attempts to address. We believe that this SAR and the proposed changes to CIP005 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511. FERC directed only that NERC provide additional guidance, beyond that provided in the version 1 standard and frequently asked questions, as to what constitutes "strong authentication". This could be accomplished through a guidance document, or the addition of a definition for "strong authentication" to the NERC glossary of terms, rather than a change to the standards.</p>
Eric Ruskamp	Lincoln Electric System	6	Negative	<p>Although LES believes the scope of the proposed project addresses a valid reliability need, the language of the standard as currently drafted lacks sufficient clarity for approval. LES recommends further consideration be given to industry concerns prior to moving forward with the proposed revisions.</p>
Daryn Barker	Louisville Gas and Electric Co.	6	Negative	<p>Comments of E.ON U.S. On Negative Vote on Project 2010-15</p> <p>R6.1.2 Are the requirements stated here different from those defined in CIP-004 R4? If not, we would suggest removing this requirement.</p> <p>R6.1.3 Again, are these requirements different from those stated in the existing CIP-004 R4? If so, these differences (i.e., additional requirements) should be noted and clarified.</p> <p>R6.2</p>

Voter	Entity	Segment	Vote	Comment
				<p>E.ON U.S. suggests adding clarification to the requirement "...to ensure only authorized individuals can establish remote access to the..." so that it reads "...to ensure only authorized individuals can establish remote, external, interactive access to the...".</p> <p>R6.2.3 Is this a change to requirement CIP-005 R5.3 regarding the retention of electronic access logs? If the requirements stated here are different, then these differences should be clarified.</p> <p>R 6.3.1 By encrypting the message all the way from the remote node to the host within the ESP the ability to detect and block malicious traffic at the access point to the ESP is removed. This would necessitate the addition of host-based intrusion detection/prevention on all assets to which remote connections are being established. Host-based protection systems are generally not as robust and effective as a single- purpose appliance for detecting and blocking the widest range of threats/ attacks. E.ON U.S. believes a better solution is to use an appliance based IPS solution on the inside of the access point prior to permitting connection to a CCA device and not requiring encryption beyond the access point.</p> <p>R 6.3.2 Is this simply restating 6.1 and 6.2.1 requiring strong procedural and technical authentication controls?</p> <p>R6.4 The addition of an intermediate jump-host or proxy device actually introduces an additional set of vulnerabilities (those associated with this device) that could be attacked and compromise the Integrity of the protected ESP. Worse yet, once compromised, these could allow remote attackers access to the protected ESPs while leaving the false impression that security was actually better.</p> <p>Missing from the SAR is a clear and concise definition for "remote access". This seems to have been generally interpreted to-date as external access from outside the corporate enterprise environment. However, with CIP-</p>

Voter	Entity	Segment	Vote	Comment
				<p>011, NERC seems to be moving towards an interpretation as “any electronic access from outside the ESP”. This is a significant change if that is the intent, and could require entities to make major infrastructure and procedural modifications.</p> <p>There has been much discussion over the last several months regarding the permissible use of remote access by entities. It seems NERC has been leaning towards a stance that external, interactive, remote access is permissible (given the proper controls) for administrative or maintenance support. However, this use for remote operations (with full-control capabilities) seems to not be allowed. The SAR as written does not address this point if that is the intended position, and E.ON U.S. believes the intent should be clearly stated.</p> <p>One additional note on the SAR...one of the most ambiguous requirements discussed over the past several months regarding NERC’s guidance on remote access stated that the devices utilized to connect remotely must be documented and treated as CCA’s. This implies that these devices must also be afforded the physical security protections (i.e., the 6-wall boundary). If this physical security requirement must be met, this effectively negates the ability for any sort of “mobile device”, such as a laptop, to be utilized outside a protected security perimeter. Despite repeated attempts to have this clarified, to-date we have been unable to get an opinion on this specific point from NERC/SERC. Without this exception, the majority of use-cases for our remote access will not be permitted, making all of these additional controls unnecessary.</p>
Daniel Prowse	Manitoba Hydro	6	Negative	<p>General Comments:</p> <ol style="list-style-type: none"> <li>1. Remote Access: It is unclear whether “remote access” refers to “remote interactive access” of a person to the Cyber Asset, or remote machine-to-machine access with the Cyber Asset. Both these types of access are distinct, and have different security solutions. If the intent is to address the person to Cyber Asset access, and the machine-to-machine Cyber Asset access, then they should be addressed separately in the standard.</li> <li>2. Removal of Technically Feasible: Legacy devices may be unable to meet the prescriptive technical requirements of the proposed R6, and therefore</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>the requirements should only apply where technically feasible, and be subject to the Technical Feasibility Exception process.</p> <p>3. Version History: The standard applies to Cyber Assets, not Critical Assets. The reference to "for support staff maintenance" in the Action is not reflected in the accompanying SAR, which makes vague references to remote access. The proposed standard, as written, could be interpreted to apply to remote access for any purpose.</p> <p>R6 - The current wording is too broad. Suggest wording "The Responsible Entity shall implement the following controls before granting remote interactive access to its Electronic Security Perimeters, to prevent unauthorized access to its Cyber Assets within its Electronic Security Perimeters."</p> <p>R6.1.1 - Vendor personnel who provide technical support for Cyber Assets within the ESP should also be authorized. Suggest wording "... vendor personnel who have authorized electronic access who provide technical support ...".</p> <p>R6.2.1 - The current wording could be interpreted as requiring multifactor authentication to, and including, the Cyber Asset within the ESP. Not all Cyber Assets within the ESP will support multifactor authentication. Multifactor authentication to the ESP should be sufficient. R6.3 - The actual intent of Requirement 6.3 is unclear. Regarding the statement "Restrict the protocols ... to protocols that: Provide encrypted communications .... " Is the intent that the protocol provide the encryption? Not all protocols provide encryption, although other technologies can encrypt communications, but not at the protocol level. Is the intent that the protocol support the authentication? Not all protocols support authentication, although other technologies can support authentication. The intent of the requirement should be to require secure communications, without being overly prescriptive. The terms "remote node" and "host" are not clear, are not defined, and are not used anywhere else in CIP-003 through CIP-009.</p> <p>R6.3.1 - Requirement 6.3.1 specifies that encrypted communications must</p>

Voter	Entity	Segment	Vote	Comment
				<p>terminate at a host within the ESP. VPN tunnels that terminate at a firewall provide the same or a better level of security as VPN tunnels that terminate at an internal proxy server, are a mainstream IT architecture and should not be excluded. This architecture also has the advantage of supporting unencrypted traffic within the ESP, which allows the firewall's anti-malware software and the IDS sensors inside the ESP to analyze the traffic. The current wording excludes this architecture. R6.4 - The wording, the intent, and the security value of Requirement 6.4 is unclear and this requirement should be removed.</p>
Dennis Kimm	MidAmerican Energy Co.	6	Negative	<p>1. Proposed R6 replaces R2.4's reference to "external interactive access" with "remote access." "External interactive access" should be retained, consistently referenced throughout CIP-005 in all applicable requirements and defined locally in only CIP-005 as follows: "External interactive access is defined as network access using routable protocol initiated by an end user outside the ESP to remotely control or access a console or terminal based session on another network attached device inside the ESP."</p> <p>2. Proposed R6 prescribes "how" to comply and "what is required." For example, encryption is "how" versus "protect communications" would be "what." Similarly, requiring an intermediate device or system is "how" not "what." Proposed R6.2.1 requires "multifactor authentication" and replaces existing R2.4 "strong controls." Strong controls is "what" whereas "multifactor" is "how" and undefined.</p> <p>3. Proposed R6.3.1. requires encryption to the host inside the ESP. This is not correct. If encryption is required, it should be to "provide encrypted communications between the remote node to the access point and be available for inspection within the ESP."</p> <p>4. Proposed R6.1.1.-.3 overlap the remaining new CIP-005 R2.4 and requirements in CIP-004 and CIP-007 R5. Proposed R6.2.2 overlaps CIP-007 logging and alerting. Redundancy should be eliminated.</p> <p>5. Proposed R6.1.2. creates a definition for annual unique to this one requirement. This is unacceptable. A universal definition of annual for all CIP should be adopted through the standard SAR process.</p> <p>6. Proposed R6.2.2 requires documenting duration of remote access. This is contradictory to the approaches for logs in CIP-006 and -007. Should</p>

Voter	Entity	Segment	Vote	Comment
				<p>proposed R6.2.2 be addressed with existing CIP-005 R3?</p> <p>7. Overall the proposed revisions create additional undefined terms, prescribe "how" not "what" and introduce confusing redundancy/overlap to other existing standards. Existing R2.4 and R2.5 should be enhanced minimally to achieve the desired result.</p>
Joseph O'Brien	Northern Indiana Public Service Co.	6	Negative	<p>General Comments</p> <ol style="list-style-type: none"> <li>1. <b>NIPSCO</b> would like a concise definition of what the scope of remote access is. Is remote access explicit to the source of the communication; Internet, corporate network, or anything outside the ESP? Does remote access include ESP-to-ESP communications? Is remote access explicit to a type of communication; application to application non interactive communication, system to system non interactive communication, or specifically administrative interactive access? In order to ballot on the addition of a remote access requirement, a definition and scope need to be provided for the term remote access.</li> <li>2. NIPSCO recommends that the drafting team consider a longer implementation plan. The changes that may be required would be difficult to implement in the larger, more complex environments in such a short period of time. The drafting team needs to consider the processes required for implementing changes to existing entity environments (e.g. purchasing hardware, change management, documentation updates, testing, potential non-compliance issues as entities implement changes to existing critical environments, etc.), and recognize that it would be extremely difficult to implement in a six to nine month period. NIPSCO recommends extending the implementation plan to 12 – 18 months.</li> <li>3. The modifications to this CIP-005 standard are often related to numerous other CIP standards. NIPSCO recommends striking the entire CIP-005-4 R6.1 and sub-requirements. The section addresses user management and authorization of users who have authorized cyber access to critical cyber assets. NIPSCO feels that this section conflicts with CIP-004 R4 and is unnecessary.</li> <li>4. The drafting team should consider removing the entire CIP-005-4 R6 Remote Access requirements and incorporating some of the key</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>components into the existing CIP sections 2.3 and 2.4. That would entail not removing the current requirements and expanding interactive access to include remote access and it would eliminate the overlap of other CIP standards.</p> <p><b>Requirement-by-requirement issues:</b></p> <p>R6.2 – NIPSCO recommends this section to be clarified to include only interactive logins. The external interactive access language from requirement 2.3 should be added back in this requirement to clarify that remote access should only include interactive access into the ESP. In addition, NIPSCO recommends explicitly excluding non-interactive access (e.g, application-to-application, machine-to-machine) from the CIP-005 Remote Access requirements.</p> <p>R6.2.3 – The drafting team needs to clarify “retain all logs”. If ESP logs are the only required logs to be maintained, this requirement should be removed as CIP-005 R3 addresses the monitoring and logging of ESP access. If the entity were required to capture the entire path of remote access logs it would pose technical challenges, expand the scope of devices to retain logs from beyond the scope of the CIP standards, and depending on current entity technology structure this may require additional resources.</p> <p>R6.3 – Where would the encryption initiate and terminate? The drafting team needs to clarify whether it is the entire path needs to be encrypted or something less (from a VPN concentrator, from the intermediate device suggested in 6.4, to the ESP, etc this complexity will vary by entity, but the intent of the requirement needs to be clearly defined). The current wording suggests that the encryption would initiate from the desktop and terminate at the host within the ESP. NIPSCO believes this would be a major issue as it may classify hosts in your ESP as access points if they are termination points for remote access.</p> <p>R6.4 – NIPSCO believes this to be inconsistent with R6.3. It would be extremely difficult to do end-to-end encryption and use an intermediate device. The requirement needs to include language to clarify where the</p>

Voter	Entity	Segment	Vote	Comment
				<p>encryption must be utilized, or strike the requirement. In addition, the requirement to have an intermediate device as a jumping point, depending on entity implementation may or may not consider the intermediate device as a CCA. This wording will leave open the interpretation of whether the intermediate asset should be a CCA or not. Further clarification regarding what requirements would be applicable? All CIP requirements or a subset – if all then the intermediate device would be a CCA, as a CCA would be in an ESP, however as an intermediate device would need to reside in an ESP different than the native CCA ESP and you would need an intermediate device to talk to the intermediate device and so on. This requirement may go beyond the scope of the current CIP-002 standards in defining cyber assets within the scope of CIP. Further clarification around this requirement is necessary.</p> <p><b>Measures:</b></p> <p>NIPSCO recommends removing the additional measure if the requirements are realigned back under requirements 2.3 and 2.4.</p>
Alan R. Johnson	NRG Energy, Inc.	6	Negative	<p>The standard should address restricting support personnel from being able to perform certain actions, such as control. EMS system support personnel can always use tools to manipulate database parameters, allowing themselves control ability. They all have database tools that are needed to diagnose systems in times of emergency.</p>
Scott L Smith	PacifiCorp	6	Negative	<p>Regarding the deletion of CIP-005-3 R2.4, we have no objection.</p> <p>Regarding the additional material of R6, we have the following comments:</p> <p><b>R6</b> -- "Remote Access" is not defined adequately. Does Remote Access refer to "human interactive access" or does it encompass any and all network communications between a host internal to the ESP and a host external to the ESP? Is there any distinction between read only remote access and write enabled remote access? Have we abandoned the distinction between human interactive access and system to system communications?</p> <p><b>Recommendation:</b> Define "Remote Access" such that it is qualified as "human interactive access".</p>

Voter	Entity	Segment	Vote	Comment
				<p><b>R6.1</b> -- This language indicates that only two categories of individuals may be granted remote access: employees of the entity and vendor technical support personnel. This would exclude third parties who simply need to retrieve data, but are not employees of the entity nor provide technical support. For example, Cowlitz Public Utility District is a non-operator owner of the Swift No. 2 generating facility operated by PacifiCorp, and thus currently has access privileges to the site and data. Cowlitz PUD also has some access rights to data related to the Swift No. 1 facility which is owned and operated by PacifiCorp. Under the new language in R6.1, Cowlitz PUD, as a third party entity, would lose any remote access privileges, which is problematic.</p> <p><b>Recommendation:</b> Avoid categories of personnel and simply require that all remote access comply with the principle of "least privilege" or add business partner as an attribute for qualification of remote access.</p> <p><b>R6.3</b> -- This section needs a technical feasibility exception for legacy equipment that does not support encryption. For example, telnet protocol which may well be encrypted by virtue of it's traversing a VPN between the Access Point and the VPN client, but would not be encrypted between the internal host and the Access Point.</p> <p><b>Recommendation:</b> Include the phrase, "where technically feasible".</p> <p><b>R6.4</b> -- This language needs clarification. What is meant by "communicate directly"? Specifically, at what point in the OSI stack are we inserting this "barrier" to direct communication? Layer 3 (firewall - perhaps NAT/PAT)? Layer 4-7 (proxy)?</p> <p><b>Recommendation:</b> Drop this requirement completely.</p>
Mark A Heimbach	PPL EnergyPlus LLC	6	Negative	<p><b>General comments</b></p> <ul style="list-style-type: none"> <li>Define the term 'Remote Access'. Assuming 'remote access' is meant to be interactive remote access, define remotely as specifically as</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>possible.</p> <ul style="list-style-type: none"> <li>• State that 'Remote Access' means interactive access and not machine to machine access. Define as specifically as possible.</li> <li>• Remote access should not include ESP to ESP communication within Registered Entities network.</li> <li>• Some of the requirements in R6.x as written may not be technically feasible for all assets that are within an ESP that require the capability for remote communication.</li> </ul> <p><b>R2.4</b> Original requirement deleted. No comment.</p> <p><b>R6.1.1</b> The current wording in the proposed standard is covered by other standards. Additionally, this language could imply that vendor personnel do not need to be authorized by the asset owner. This sub-requirement should be removed.</p> <p><b>R6.1.2</b> The current requirement for list of accesses and review are covered by CIP-004 R4.1 and CIP-007 R5.1.3. This requirement is redundant and should be deleted. If this requirement remains, are separate authorized access lists required for remote access?</p> <p><b>R6.1.3</b> This requirement combines two activities together that are very different in nature. Verifying who has been given authorized access and if that access is still valid is covered in CIP-004 R4.1 and CIP-007 R5.1.3. This new requirement is requesting a verification of the technical implementation to ensure the remote access is secure which would be accomplished by a vulnerability assessment, similar to CIP-007 R8. Suggest this be a sub-requirement of R6.2 which states only authorized individuals can establish remote access to the ESP.</p> <p><b>R6.2</b> Define multi-factor authentication. This was done in a subsequent release of a draft Secure Remote Access document. Ensure this is finalized with</p>

Voter	Entity	Segment	Vote	Comment
				<p>the CIP-005 changes.</p> <p><b>R6.2.1</b> Clarify when use of multi-factor authentication is required. Multi-factor authentication is required when crossing the ESP to access a cyber asset. Is multi-factor authentication required when crossing into the Corporate Network?</p> <p><b>R6.2.2</b> Systems may not be capable of accurately, or meaningfully, tracking or providing duration of access, if at all feasible. Consider the need for this logging.</p> <p><b>R6.3.1</b> Clarify what traffic needs to be encrypted. Proposed language says 'encrypted communications between the remote node and the host inside the ESP' and there is no TFE mentioned. Not all 'hosts' inside an ESP are capable of supporting encryption. Can a TFE be taken? Clarify or rephrase to 'Provide encrypted communications between remote access points to the ESP access point, where technically feasible.'</p> <p><b>R6.3.2</b> This requirement is a design requirement which should be a sub-requirement of R6.2.1 if necessary at all depending upon the definition of multi-factor authentication.</p> <p><b>R6.4</b> The requirement as worded is very ambiguous. Is this intended to apply to remote interactive access by a human or a host-to-host communication?</p> <p>Consider an individual sitting in PSP 1 using multi-factor authentication to access a CCA system in ESP 1 in PSP 1 and the CCA system sends a transaction from ESP 1 to CCA in ESP 2 in PSP 2. Is this remote access as an individual initiated the transaction? Or not, because the system is making the connection, host to host? Would this transaction need to pass through a jump server? Or is R6.4 intended to mean an individual sitting in a remote location using multi-factor authentication to access a CCA system</p>

Voter	Entity	Segment	Vote	Comment
				in ESP 1 in PSP 1? More generally, is a jump server required for traffic between all assets?
James D. Hebson	PSEG Energy Resources & Trade LLC	6	Negative	<p>1) There is no definition of remote access. There needs to be an agreed to definition. Does it include interactive, human user access? Does it include computer to computer interfaces? What about access to an intermediary that in turn talks to the ESP devices? PSEG suggests that remote access for this requirement be restricted to interactive, human user access through the ESP boundary into the ESP protected network.</p> <p>2) Also needed is a definition of multifactor authentication placed in the standard rather than rely on the supporting guide document.</p> <p>3) In R.6 it should be clarified that access controls and user lists for multiple ESPs can consist of a combined control and list for all ESPs.</p> <p>4) What does "validate the record of individuals with authorized remote access" in R6.1.2 mean? Must entities validate every access attempt or only validate the list of authorized users? Please clarify.</p> <p>5) R6.1.2/6.1.3 should be incorporated as a sub requirement for R6.2 such as: "Review the list of those authorized to remotely access Cyber Assets within an Electronic Security Perimeter at least once each calendar year, with no more than 15 months between reviews and verify that access controls implemented pursuant to Requirement R6.2 only allow access to individuals authorized for that access."</p> <p>6) R6.1.1/R6.1. should be part of R6.1 and eliminate the sub requirements Suggest it be revised to read as follows: "R6.1. Establish, implement, and document procedural controls to authorize remote access to the Electronic Security Perimeter limiting access to those Responsible Entity's personnel who have authorized electronic access to those Cyber Assets and require remote access and to vendor personnel who provide technical support of the Cyber Assets within the specific Electronic Security Perimeter."</p> <p>7) R6.2.1 should be revised to (1) require multifactor authentication for remote access to the ESP but not to access CCAs inside the ESP since</p>

Voter	Entity	Segment	Vote	Comment
				<p>the latter may not be possible to implement, or provide for a TFE and (2) provide for a TFE for logging the duration of access since that is not possible with many systems and devices.</p> <p>8) R6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. It should be sufficient for the encryption to terminate at device establishing the Electronic Security Perimeter. Why does the encryption need to go all the way to the device? In some cases it may need to but there should be no general requirement that all communications within an ESP be encrypted. This requirement is too prescriptive and should be clarified to indicate it allows the encryption to end at the access point to the ESP.</p> <p>9) R6.4. Should provide for a TFE for systems or software that do not support the use or relay or proxy systems that appears to be required as now written.</p>
Trent Carlson	RRI Energy	6	Negative	<ol style="list-style-type: none"> <li>1. NERC needs to explicitly define "remote access" for this standard. We believe that remote access is an individual using a cyber asset outside the Electronic Security Perimeter to login and connect to a Cyber Asset within the Electronic Security Perimeter. We do not believe that remote access is an application server (i.e. such as an EMS server) collecting data from a plant device (example: RTU) within the Electronic Security Perimeter.</li> <li>2. Requirement R6.3.1 needs clarification. More specifically, NERC needs to define "remote node" and to define "host". We believe that the remote node is most likely the "intermediate device" required in R6.4 and the host is a cyber asset within the Electronic Security Perimeter.</li> <li>3. Requirement 6.4 should read: Implement an intermediate device or system such that the external system used for remote access does not communicate directly with a Cyber Asset within the Electronic Security Perimeter. Additionally, "external system" should be defined as cyber asset used by an individual to log into and connect to the intermediate device for the purpose of subsequently logging into a cyber asset within the Electronic Security Perimeter.</li> </ol>

Voter	Entity	Segment	Vote	Comment
Dennis Sismaet	Seattle City Light	6	Negative	While we agree with the majority of the changes recommended by the Standard Drafting Team, we nevertheless voted negative because of Requirement 6.3.1. Provide encrypted communications between the remote node and the host inside the Electronic Security Perimeter. First, we do not believe this requirement will effectively enhance security. Specifically, by forcing end-to-end encryption for remote communications but not for sessions that originate locally provides little security benefit if you leave internally-sourced sessions in the clear. We are unaware of any other regulatory frameworks that require end-to-end (host-to- host) encryption, including PCI and HIPAA. Normal practice is to terminate encryption at the gateway. Further, this proposal introduces key management issues and could introduce operational issues if encryption fails and connections are not possible. This model introduces more points of failure. Finally, we believe this requirement will be very difficult to accomplish on any widespread basis.
Marjorie S. Parsons	Tennessee Valley Authority	6	Negative	<p>Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this USAR. We fully support the standards development process and all the hard work and commitment by the USAR team members. For this USAR, we have the following concerns which moved us to cast a Negative vote. General Comments:</p> <ol style="list-style-type: none"> <li>1. There isn't a clear definition of the term "remote access." Without this definition there are many ways to interpret this standard. This lack of clarification makes it very difficult to frame questions associated with these proposed new requirements. For example, is communications from a Responsible Entity's non-ESP into their ESP considered remote access? Is communications between a Responsible Entity's ESP's considered remote access, see General Comment #2? Recommendation: For the purpose of this standard define remote access something like, access originating outside any defined and trusted ESP from a remote location through a data link not controlled by the Responsible Entity, explicitly excluding all Responsible Entity's Inter-ESP communications (e.g. ESP to ESP communications) and non-ESP to ESP communications.</li> <li>2. Inter-ESP communications. Without remote access being clearly defined, it isn't clear if Inter-ESP communications is considered remote access. Does this require every ESP to contain an intermediate device or system for</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>remote access? In an environment that has multiple ESP's located on a private network can there be one access point. For example, an organization that has 50 substations that are interconnected on a private network. There is an ESP at each substation with a remote access point being centralized at a control center. Is there an expectation that communication between the control center and the substations, separate ESP's, take place over encrypted communication? Recommendation: Inter-ESP communications is outside the scope of this requirement. Communications between two defined and trusted ESP's isn't considered Remote Access. This would imply there is a "mutual trust" between ESP's owned and managed by the Responsible Entity.</p> <p>Specific Comments:</p> <ol style="list-style-type: none"> <li>1. 6.1 - This requirement focuses on account management which is already addressed in other standards. Recommendation: To ensure consistency across the standards we recommend that the same verbiage in CIP-007 R5 is used in this section.</li> <li>2. 6.3.1 - The way this requirements is worded makes it sound like encrypted communications must be used between the remote node and each individual device it is communicating with within the ESP. This isn't technically feasible. Recommendation: Reword the requirement to make it clear that encryption is only required between the remote node (end-user device (e.g. laptop)) and the gateway into the ESP (e.g. VPN Access Point).</li> <li>3. 6.3.1 - It is unclear if language reference to "the host" means the cyber asset within the ESP versus an intermediate device or system as described in 6.4. Recommendation: Reword 6.3.1 and 6.4 to provide more clarity.</li> </ol>
Roger C Zaklukiewicz		8	Negative	<p>My negative vote is based upon: There is no proposed corresponding implementation plan. Need clarification of the term "remote access" in R6. Suggest replacing with "remote interactive access to Cyber Assets in the ESP from outside of teh ESP". The SAR should use the defined term CYBER ASSET rather than the term "devices" which is not defined. The updates to CIP-005 do not respond to the SAR's intended purpose of end point protection. The updates address the protection of the Electronic Security Perimeter (ESP). The new R6 should replace the stricken R2.3. The</p>

Voter	Entity	Segment	Vote	Comment
				language of R6 should be clarified to more accurately reflect the intended scope of the SAR. Remove R6.1 since it duplicates the Requirements within CIP-004. Remove R6.2 as it duplicates the Requirements within CIP-007. Remove R6.3 as it duplicates the ports and services requirements within CIP-005 R4.2.
Nicholas Lauriat	Network & Security Technologies	8	Negative	<ul style="list-style-type: none"> <li>- The definition of "remote access" is vague. If it is intended to mean access by users whose own Cyber Assets are outside the ESP and have the ability to view and/or manipulate data on one or more Cyber Assets within the ESP, this should be made explicit. We suggest retaining the now deleted term, "external interactive access."</li> <li>- We understand, based on language in the SAR for this update and from comments about the update by presenters at the Denver, CO CIPC meeting, that the new requirements for remote access are intended to apply only to remote access from user systems that (a) are used only for maintenance purposes and have no BES control capabilities, and (b) are therefore not themselves Critical Cyber Assets. However, as presently written, we believe the proposed revisions to CIP-005 could be interpreted to apply to any and all remote systems, including CCAs in other ESPs. We believe this should be corrected, and that R6 should clearly indicate it applies only to Cyber Assets that are not CCAs, are not inside a CIP-005 compliant ESP, and can be used only for maintenance purposes.</li> <li>- We consider the new requirement to use encryption for remote access connections subject to proposed requirement R6 to be inappropriately prescriptive, and we recommend it be replaced by a requirement to implement a procedural and/or technical solution to whatever cyber security problem(s) encryption is intended to address (e.g., host authentication, data confidentiality, data integrity).</li> <li>- We consider R6.3.1 (encryption between the remote node and the host inside the Electronic Security Perimeter) and R6.4 (intermediate device or system) to be contradictory requirements unless it is NERC's intention to require the use of two concatenated encrypted connections, one from the remote Cyber Asset to the intermediate device and one from the intermediate device to the destination Cyber Asset inside the ESP. Such an arrangement would likely be difficult to</li> </ul>

Voter	Entity	Segment	Vote	Comment
				<p>implement and manage, if feasible at all, and could also result in unacceptably poor performance. Moreover, a requirement to use encryption between the remote node and the host inside the Electronic Security Perimeter could hamper an entity's ability to use network-based intrusion detection or prevention as a protective mechanism inside the ESP. We believe encryption, if required, should only be required between the remote Cyber Asset and the intermediate device or system.</p> <p>- R6.3.1 uses two terms, "node" and "host," that are not used anywhere else in CIP Standards 002 through 009. We recommend replacing both with "Cyber Asset."</p>
Donald E. Nelson	Commonwealth of Massachusetts Department of Public Utilities	9	Negative	<p>There is no proposed corresponding implementation plan The industry did not have an opportunity to request clarification on what "remote access" means to provide a more accurate scope for the SAR. What type of remote access? What is this SAR trying protect? Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)," We believe that Cyber Asset can include smartphones like Blackberry. The updates to CIP-005 do not respond the SAR's intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP) Recommend that the new R6 should replace the stricken R2.3 since not moving R6 creates the possibility of violating two Requirements or double-jeopardy. Recommend clarifying "remote access" in R6. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP" Recommend that the language for R6 be clarified to more accurately reflect the intended scope, specifically to the following:</p> <p>o Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</p>

Voter	Entity	Segment	Vote	Comment
				<p>o CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</p> <p>o It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer. Recommend removing R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy Recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2. There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural, putting this under technical requirements implies that only technical solutions are acceptable. Recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2 Do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>
Diane J. Barney	National Association of Regulatory Utility Commissioners	9	Negative	Discussions I have seen indicate that there is not a clear definition as to either "devices" or "remote access"; these terms need to be defined for the standard to be enforceable.

Voter	Entity	Segment	Vote	Comment
Jerome Murray	Oregon Public Utility Commission	9	Negative	The proposed changes do not contribute substantively to the current version of CIP-005. Also the proposed revisions should indicate "what" is required rather than "how" to comply. For example, Requirement R6.3.1 requires encryption between the remote host and the host within the Electronic Security Perimeter (ESP). The requirement should require that communications from the remote host to the access point to the ESP or intermediate device should be protected from tampering. Encryption is one method but others should be allowed if they can ensure confidentiality and integrity. Further, the proposed standard may cause confusion between or be inconsistent with other existing CIP standards. For example, R6.1.1 limits access to specific entities while CIP-004, R4 requires a list of authorized personnel. There is also no definition of "remote access" in the proposed standard.
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Negative	<p>There is no proposed corresponding implementation plan The industry did not have an opportunity to request clarification on what "remote access" means to provide a more accurate scope for the SAR. What type of remote access? What is this SAR trying protect? Why does the SAR's Brief Description use "devices" instead of the defined term Cyber Asset? "A Requirement will be added to CIP-005-3 that describes requirements placed on a) the devices used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter)," We believe that Cyber Asset can include smartphones like Blackberry. The updates to CIP-005 do not respond the SAR's intent of end point protection. The updates speak to protecting the Electronic Security Perimeter (ESP) Recommend that the new R6 should replace the stricken R2.3 since not moving R6 creates the possibility of violating two Requirements or double-jeopardy. Recommend clarifying "remote access" in R6. Instead of "remote access" suggest using "remote interactive user access to Cyber Assets in the ESP from outside of the ESP" Recommend that the language for R6 be clarified to more accurately reflect the intended scope, specifically to the following:</p> <p>o Sub-requirements of R6 indicate that R6 intends to allow remote interactive user access only for the purpose of maintenance and support and disallows it for any other purpose: is it the intent? If so, recommend that the language be in the overall R6 paragraph, not as a sub-requirement.</p>

Voter	Entity	Segment	Vote	Comment
				<p>o CAN-005 appears to allow remote interactive user access for operations and control of Critical Assets as long as the accessing Cyber Asset is designated as a Critical Cyber Asset. This is in direct contradiction with R6 as it stands now.</p> <p>o It is not clear whether requirement R6 is intended to apply for Cyber Assets accessing the ESP for maintenance and support only, or to any remote interactive user access, whatever the purpose. The requirement and sub-requirements in the current R6 appear to be just as applicable for protection of any kind of remote interactive user access. The language in the version history log seems to be clearer. Recommend removing R6.1 since it duplicates CIP-004 Requirements which creates double jeopardy Recommend removing R6.2 since it duplicates CIP-007 Requirements and CIP-005 R1.5 and R2. There is no official definition of multifactor authentication in R6.2.1. Multifactor authentication can be technical or procedural, putting this under technical requirements implies that only technical solutions are acceptable. Recommend removing R6.3 since it duplicates the ports and services requirements in CIP-005 R4.2 Do not agree with R6.3.1 because adding encryption at the access control point removes visibility with respect to security Remove R6.4 because this Requirement is prescriptive, telling how to implement. The Requirement should identify what the target is or what is the desired end result.</p>
Carter B Edge	SERC Reliability Corporation	10	Negative	<p>Generally, these revisions are headed in the right direction but have issues of clarity, redundancy, and depth. Below are changes we are suggesting that, if addressed, would result in a "yes" vote.</p> <ol style="list-style-type: none"> <li>1. For requirement R6, we agree with the direction but request clarifying information regarding the term "remote access". Beyond remote user interactive access into ESP, does this also include ESP-to-ESP communication (e.g. network-to-network IPSEC VPN), any application-level access into the ESP (e.g. corporate web server to an EMS database), etc?</li> <li>2. For requirements R6.1.2 and 6.1.3, we agree with the overall direction of the root requirement but feel these are redundant as part of the access list structure already in CIP-004 R4 and easier to accommodate</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>within CIP-004 R4 as a "callout" instead of creating another separate list requirement with different timing.</p> <ol style="list-style-type: none"> <li data-bbox="1003 334 1892 586">3. For requirement 6.3, we agree with the direction but request clarifying information regarding "protocols" as it quickly goes into sub-requirements not about ports per se. It is unclear if the intent is to restrict the ports to be only those in the the sub-requirements or if it is meant to state something like "restrict ports and services only to those required for remote access" (i.e. VPN tunnels should be locked down to only allow the remote access protocol e.g. only open port 3389 for terminal services.</li> <li data-bbox="1003 621 1892 841">4. For requirement 6.3, we agree with the existing set of sub-requirements but request additional sub-requirements around the remote access host itself. The examples of these remote host controls might include, but is not limited to: a local firewall on the remote host that cannot be disabled by default; prohibiting split-tunnel VPN; anti-virus cannot be disabled by default and is up to date; and limited file-sharing between remote host and remote destination.</li> <li data-bbox="1003 876 1892 1096">5. For requirement 6.4, we agree with the direction but request clarifying information regarding on "intermediate access". This appears to be addressed in the supplemental guidance document "Secure Remote Access" but should be better associated by adding language such as "including VPN servers and proxy server. Interactive access shall require a jump host". The use of "or" indicates either is acceptable but interactive examples all show a jump host.</li> <li data-bbox="1003 1131 1892 1320">6. All new terms and phrases which are not currently defined in the NERC glossary and are not in accordance with generally accepted terminology (found in an English dictionary or in another CIP standard) should be explicitly defined, either in this standard or in the NERC glossary. Failure to define these terms in other standards has led to significant numbers of possible violations and confusion.</li> </ol>

Voter	Entity	Segment	Vote	Comment
Stacy Dochoda	Southwest Power Pool Regional Entity	10	Negative	<p>1) R6.1.1 in effect does away with the requirement for a completed Personnel Risk Assessment and annual security training for vendor support personnel. The PRA and training should continue to be required and the emergency provisions of CIP-003, Requirement R1 should be used when the PRA and/or training is truly impractical.</p> <p>2) R6.1.2 requires the entity to “maintain” a record of all individuals authorized for remote access to Cyber Assets within an Electronic Security Perimeter and to “validate” the record of individuals with authorized remote access at least once each calendar year. It is not clear what this record is or how the entity would validate it. How does this requirement compare to access list maintenance and review requirements of CIP-004, Requirements R4 and R4.1?</p> <p>3) R6.1.3 is not enforceable. There is no reasonable method to ensure that someone granted remote access does not then hand over control to an unidentified person. Once a remote session is started, it is not always possible to monitor who is actually using the access session.</p> <p>4) R6.2.3 makes an oblique reference to the three-year log retention requirement of CIP-008, Requirement R2, but uses the language “as long as necessary to support an investigation of a cyber security incident pursuant to CIP-008.” Suggest changing the statement to read “Retain all logs specified in Requirement R6.2.2 for a minimum of ninety calendar days unless longer retention is required pursuant to the current version of Standard CIP-008, Requirement R2.”</p> <p>5) R6.3.1 as written allows a remote system to bypass all of the firewall, Intrusion Detection and Intrusion Prevention protections by requiring an encrypted session directly between the remote node and the host inside the Electronic Security Perimeter. This is typically achieved using a VPN tunnel. Because the traffic is encrypted, there is no possibility of a deep packet inspection to look for malware signatures or other signs of cyber attack. This exposes the target host within the Electronic Security Perimeter to compromise and exploitation. Good security practice terminates the encrypted session within a DMZ outside of the perimeter access control systems (firewalls, etc.) and requires the</p>

Voter	Entity	Segment	Vote	Comment
				<p>session traffic to be authenticated into the protected networks.</p> <p>6) R6.4 is confusing and may conflict with the provisions of R6.3.1. I think the drafters are suggesting the use of something like a Citrix server where the remote PC/laptop connects to the Citrix server and it is actually the Citrix server that is communicating with the target host within the ESP. Ideally, the Citrix server would sit outside of the ESP, but the location of the intermediate system on the network is not defined in the requirement. Especially confusing is the reference to not communicating directly with a Cyber Asset. The intermediate system is most likely a Cyber Asset by definition, making the use of this terminology nonsensical as written.</p>
Louise McCarren	Western Electricity Coordinating Council	10	Negative	<p>We support the development of this Standard. However, we are unable to vote to approve the standard as drafted. We believe that the work to date is a good start but it needs significant improvement and continued work. The wording must be refined and clarified to add a few requirements that result in better protections by defining “strong procedural controls” as including access via a proxy, and encrypting communications used for remote access. We support the development of this Standard. However, we are unable to vote to approve the standard as drafted. We believe that the work to date is a good start but it needs significant improvement and continued work. The wording must be refined and clarified to add a few requirements that result in better protections by defining “strong procedural controls” as including access via a proxy, and encrypting communications used for remote access. Specific comments and suggestions are provided below.</p> <ol style="list-style-type: none"> <li>1. “Remote access” is not defined. This does not add any clarity but will only cause more confusion and require interpretation requests. At the root level “remote access” needs to be defined or put into context, e.g. “If a Responsible Entity allows operations, monitoring, viewing and/or network administration of cyber assets within the Electronic Security Perimeter from any device that resides outside of the Electronic Security Perimeter, that entity shall implement the following control prior to granting such authorized access:”</li> <li>2. R6.1.1 might cause confusion with CIP-004 R4 which requires that anyone with access be maintained on a list. The confusion is that 6.1.1 seems to differentiate between people on these lists</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p>(“authorized”) versus vendors support. Additionally, a reference to completion of Personnel Risk Assessment (CIP-004 R3) and Training (CIP-004 R2) should be included at a minimum. This is the riskiest type of access that exists within the information security environment.</p> <ol style="list-style-type: none"> <li>3. R6.1.2 requires that the access lists be reviewed “yearly” and no longer than 15 months, yet CIP-004 R4 requires the lists be reviewed quarterly and updated within 24 hours or 7 days of changes. Is this double jeopardy or redundant? R6.1.2. should be consistent with the requirement of CIP-004 R4. Authorized access validation is critical to protecting against loss of confidentiality and integrity. The more often that access is reviewed the better.</li> <li>4. R6.1.3 could be more clearly stated “Perform reviews to ensure that implemented access on the system corresponds to the authorized record.</li> <li>5. R6.2.2 Justification of the access attempt and subsequent success or failure of such attempt should be accounted for. Log “why” someone was on the system remotely.</li> <li>6. R6.2.3 This is inconsistent with CIP-008 R2. Retention should map to the other Standard Requirements.</li> <li>7. R6.3.1 Encryption within the Electronic Security Perimeter should not be a requirement. Encryption to the ESP access point should be a requirement. R6.3.1 requires encryption between the remote host and the host within the ESP. This will prevent inspection of the content inside the ESP by security devices such as Intrusion Detection Systems. This should require that communications from the remote host to the access point to the ESP or the intermediate device should be protected from tampering or inspection (shouldn’t specifically require encryption if other methods can ensure confidentiality and integrity).</li> <li>8. R6.3.2 seems redundant to R6.2 despite the reference back to R6.1.</li> <li>9. R6.4 should be rewritten to state that the remote host should only be allowed to access an intermediate host. Communications to this intermediate host shall be protected for confidentiality and integrity. Access to the ESP shall be restricted to this intermediate host thereby limiting remote access to the ESP to only communications through this host. “The entity shall implement intermediate devices and systems as well as procedures that preclude direct access to a cyber asset within</li> </ol>

Voter	Entity	Segment	Vote	Comment
				the Electronic Security Perimeter by a cyber asset outside of the Electronic Security Perimeter.”
Christine Hasha	ERCOT			<p><b>ERCOT Comments for CIP-005-4</b></p> <p><b>General:</b> <b>COMMENT:</b></p> <ol style="list-style-type: none"> <li>1) Some entities may have to remove remote access capabilities to comply with these requirements. This diminishes the entity's ability to respond to problems in a timely manner due to the time required to travel to the physical location of the equipment. This could have a severe negative impact on reliability. Further, many entities have implemented remote access technologies as a means to address pandemic planning as well as operations in adverse weather.</li> <li>2) Request that the drafting team write the requirements to address the principles of sound remote access capabilities rather than being prescriptive as to how an entity should achieve compliance with the requirement.</li> <li>3) Request clarification that remote access under this requirement only pertains to user-to-system access. System-to-system and program-to-system access are outside the scope of this requirement.</li> <li>4) ERCOT ISO requests a definition of “remote access”. This is a new term. The term previously used was “external interactive access”. Recommended definitions:  Remote Access: The ability for a person to log in to a computer or network within an organization from an external network not under the Responsible Entity's administrative control.  Remote Access Control System: A system designed to provide secure, authenticated communications across an insecure or untrusted network to a Responsible Entity's external network</li> </ol>

Voter	Entity	Segment	Vote	Comment
				<p data-bbox="1100 238 1220 263">boundary.</p> <p data-bbox="1003 303 1203 328"><b>Effective Date:</b></p> <p data-bbox="1003 336 1890 425"><b>COMMENT:</b> As these changes may result in significant changes to infrastructure for some organizations, request a longer implementation period than approximately nine months from effective date.</p> <p data-bbox="1003 433 1890 555">Implementation of new infrastructure may have significant costs that have not been identified for 2011 budgeting. Other entities may have to increase 24x7 on-site support to address issues that arise. Funding of these efforts may require that funds be diverted from other reliability-related efforts.</p> <p data-bbox="1003 596 1203 620"><b>Requirements:</b></p> <p data-bbox="1003 628 1890 750"><b>R6. Recommend the following revision.</b> "Responsible Entities requiring remote access to Cyber Assets within an Electronic Security Perimeter shall implement the following controls before permitting remote access to prevent unauthorized access through the Electronic Security Perimeter."</p> <p data-bbox="1003 790 1890 880"><b>R6.1. Recommend the following revision.</b> "Define, implement, and document procedural controls that establish an authorization and authentication process for remote access that include the following."</p> <p data-bbox="1003 920 1890 1042"><b>R6.2. Recommend the following revision.</b> "Define, implement, and document technical controls that ensure only authorized user accounts are permitted for remote access via the use of a Remote Access Control System."</p> <p data-bbox="1003 1083 1890 1229"><b>R6.2.1. COMMENT:</b> Request the definition of "multifactor authentication" in the Secure Remote Access reference document be adopted and added to NERC glossary of terms. <b>Recommend the following revision.</b> "Require the use of <u>M</u>ultifactor <u>A</u>uthentication for authorized users to access the Remote Access Control System."</p> <p data-bbox="1003 1269 1890 1359"><b>R6.2.2. COMMENT:</b> Request clarification of how an entity address systems that do not support logging of one or more of (1) user identification and (2) the time and duration of remote access?</p> <p data-bbox="1003 1367 1890 1416"><b>Recommend the following revision.</b> "Implement and document an electronic or manual process(es) for monitoring and logging remote access</p>

Voter	Entity	Segment	Vote	Comment
				<p>through the remote access control system twenty-four hours a day, seven days a week. Logging shall include:</p> <ol style="list-style-type: none"> <li>1. The user account;</li> <li>2. The start time of the remote access session; and</li> <li>3. The end time of the remote access session.</li> </ol> <p><b>R6.2.3. COMMENT:</b> The language should be consistent with R5.3. <b>Recommend the following revision.</b> "Retain all logs specified in Requirement R6.2.2 for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of CIP-008-3."</p> <p><b>R6.2.4. COMMENT:</b> Move R6.1.3 here. <b>Recommend the following revision.</b> "Annually, verify and document that access controls implemented pursuant to Requirement R6.2 allow access only to authorized user accounts."</p> <p><b>R6.3. COMMENT:</b> Managing this by protocol is burdensome if remote access is not clarified to only address user access and not system-to-system access or program-to system access. Recommend the following revision: "Provide encrypted communications between the authorized user's remote system and the Remote Access Control System." Remove requirements R6.3.1 and R6.3.2.</p> <p><b>R6.3.1. COMMENT:</b> As written, this requirement will render IDS and IPS systems useless to monitor communications within the network. Some applications will not support encryption (i.e.: database admin querying a database). <b>Recommend moving this to R6.3.</b></p> <p><b>R6.3.2. COMMENT:</b> This requirement appears to be redundant to 6.2.1. Recommend removing this requirement.</p> <p>10. <b>R6.4.</b> Request a definition of "intermediate device or system" since this is a new term.</p>