

Consideration of Comments on Initial Ballot — Urgent Action Revisions to CIP-005-3 (Project 2010-15)
Date of Initial Ballot: December 2-11, 2010

Summary Consideration:

Many commenters requested the reinstatement of the nuclear exemption language, which has been re-inserted.

Commenters expressed concern that the new requirement is unnecessary or duplicative of the existing requirement R2.4. The Drafting Team developed the new requirement R6 as a response to the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, not in response to any specific language in the FERC order. Further, the Drafting Team noted that the US Government expressed concern over insecure remote access configurations as expressed in that bulletin; therefore, requirements concerning remote access are necessary.

Commenters expressed concern about the definition of which Cyber Assets can initiate interactive remote access, and what this interactive remote access is allowed to be used for. The definitions have been modified to remedy these issues.

Commenters expressed concern that the new Requirement R6 was too proscriptive. The Drafting Team believes that it has provided sufficient detail for proper implantation, while allowing flexibility.

Many commenters commented on the double-jeopardy issues associated with Requirements R6.3 and R6.4. These have been extensively re-written to address these issues.

Commenters expressed concern over double jeopardy and enforcement capability for Requirement R6.5. This requirement has been re-written to address these issues.

Commenters expressed concern about the definition of which Cyber Assets can initiate interactive remote access, and what this interactive remote access is allowed to be used for. The definitions have been modified to remedy these issues.

Commenters requested more than 6 months to implement the requirements. Suggested timeframes ranged from 12 to 18 months. The Drafting Team has modified the implementation timeline to be consistent with the “Version 4” implementation timeline recently approved by industry.

Commenters expressed concern that guidance documents would be used to measure compliance. The Drafting Team responded that only Requirements in Standards can be used to assess compliance. Guidance documents are not enforceable.

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.¹

Voter	Entity	Segment	Vote	Comment
-------	--------	---------	------	---------

¹ The appeals process is in the Reliability Standards Development Procedure: http://www.nerc.com/files/RSDP_V6_1_12Mar07.pdf.

Voter	Entity	Segment	Vote	Comment
Rodney Phillips	Allegheny Power	1	Negative	Allegheny Power is not voting in favor of this standard due the following issue. This standard should not duplicate requirements from other standards, but rather reference those requirements.
<p>Response: Thank you for your comments. Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
Kirit S. Shah	Ameren Services	1	Negative	<ul style="list-style-type: none"> • The language in R6 quoted here “(or the Cyber Assets comprising the Electronic Security Perimeter’s access points)” adds to the intended scope of R6 and this late addition to the proposed standard needs to be removed. This would increase the scope of this requirement beyond its intended audience and implies the need for an intermediary device to protect access to the firewall itself. • In R6.1, the words “outside the control of the Responsible Entity” need to be added after “Cyber Assets”. This addresses the different security requirement provisions for access (such as intermediary devices) from computers located on internal corporate networks that already have strong protections from external sources in place. • We have a significant concern about the policy language in R6.5. Responsible Entities should only have to provide the policy and signed agreements, and not be expected to provide evidence of policy compliance for third parties. Please consider wording revisions to provide additional clarity.
<p>Response: Thank you for your comments. The SDT agrees with recommendations regarding R6 and the parenthetical phrase has been removed. The definitions have been modified in response to this and other comments.</p> <p>The mandatory CIP Standards only make a distinction between Cyber Assets located within an ESP, and all other Cyber Assets. Since the standards do not place any other requirements on Cyber Assets not within an ESP, all Cyber Assets not located within an ESP are treated identically. Given this, the phrase “outside the control of the Responsible Entity” cannot be inserted.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				

Voter	Entity	Segment	Vote	Comment
Paul B. Johnson	American Electric Power	1	Negative	<p>AEP does not support R6.1 as this is a very specific requirement (stating “how” to comply) and mandates a solution. Furthermore, this requirement may not provide security benefits and could introduce complexities that might be detrimental to security and/or reliability. The requirement must allow for a TFE as there are system and/or applications that do not function with a “proxy system”. There should not be a requirement that has known challenges that may require a TFE. The requirement should be broadened to allow for a variety of innovation and solutions. For example, limiting ports and services or limiting certain hardware that can connect through the ESP could be viable solutions opposed to mandating proxy servers that might not be compatible with the CCA environment. Furthermore, the proxy server configuration might be in conflict to locking down the ports and services.</p> <p>With respect to R6.3.2, CIP-004 R4 already requires the Responsible Entity to maintain and review a list of personnel with authorized cyber access. This is double jeopardy or redundant and overlapping requirement that adds no value and should be removed.</p> <p>AEP contends that R6.5 and applicable sub-requirements are paperwork related requirements that do not provide a consummate level of security benefits and therefore should be removed. There is significant risk that auditors will require evidence that the referenced controls are implemented rather than rely upon the signed policy/agreement by the end user.</p> <p>R6.5.1 - This requirement is assuming a traditional "blacklisting" anti-malware application is being used. "Whitelisting" applications have shown to be as secure as effective or more effective in preventing malware infections. Suggest changing the wording to "software or signatures", this should allow the use of "whitelisting" style applications that do not require signature updates.</p>
Raj Rana	American Electric Power	3		
Edward P. Cox	AEP Marketing	6		
<p>Response: Thank you for your comments. Information provided by the US Government and included in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)”, published in March 2010, lead to concerns expressed over insecure remote access configurations; therefore, requirements concerning remote access are necessary. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p> <p>The SDT has attempted to balance the “what” issues with the “how” issues, and feels that the proposed standards (as modified in response to comments) provides a set of requirements, with sufficient flexibility in implementation.</p>				

Voter	Entity	Segment	Vote	Comment
<p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The concept of “whitelisting” is under consideration by the Project 2008-06 SDT for future revisions to the standards.</p>				
Jason Shaver	American Transmission Company, LLC	1	Negative	<p>ATC has several concerns with the changes made to the Standard within Requirement 6 and requests that the SDT address our comments prior to issuing the final draft of CIP-005.(see Comment Form for details)</p> <p>Also, ATC feels strongly that six months is inadequate time to become compliant with the new requirements considering we need to develop a new policy, design the control systems, develop procedures, and communicate to all personnel including vendors, contractors, and consultants. In addition, we are very concerned as to how the policy would be monitored and enforced. These issues require at least a 12 month implementation period.</p>
<p>Response: Thank you for your comments. Please see the Drafting Team’s responses in the comment form response document.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
Robert D Smith	Arizona Public Service Co.	1	Negative	<p>AZPS has concerns about consistency with the rest of the CIP v4 standards as well as with some portions of the proposed requirements, including:</p> <p>1) The Applicability Section 4.2 must be aligned with the rest of the CIP v4 Standards in order to avoid significant applicability conflicts and confusion.</p> <p>2) The definition of Remote Access (next to R6), which includes user interactive access "for monitoring, support, and maintenance", appears to exclude remote system operator consoles or other business uses not covered by CAN-0005. AZPS considers this apparent gap considerable and recommends that the remote access use not be constrained - the act of remote access incurs risks that must be addressed, irrespective of</p>
Steven Norris	APS	3		
Mel Jensen	APS	5		

Voter	Entity	Segment	Vote	Comment
				<p>the purpose or nature of the access.</p> <p>3) The encryption requirement in R6.2 appears to be unnecessarily narrow, only focusing on networks outside of the Responsible Entity's control. AZPS considers there to be considerable risks even on networks that the REs do control and that requiring encryption up to the ESP access point is not an undue burden. AZPS recommends modifying the requirement to include encryption up to the ESP access point.</p> <p>4) R6.3.1 appears to restrict authorized users to RE personnel and vendors, while the definition of Remote Access for R6 includes the additional concepts of contractors and consultants. AZPS considers this requirement to be unnecessarily restrictive and redundant (to R2.4 and R6.3.2), and recommends that this requirement be removed.</p> <p>5) R6.3.2 appears to create ambiguity in reference to CIP-004-4 R4 reviews. It is not clear if the 'in accordance with' review requirement is restricted to the literal text of CIP-004-4 R4 alone (e.g. excluding R4.1 and R4.2) or if the intent is to include the R4.1 and R4.2 sub-requirements of quarterly reviews and 7-day/24-hour revocations. AZPS recommends that the 'in accordance with' reference be strengthened to include specifically which portions of CIP-004-4 R4, R4.1 and/or R4.2 are intended.</p> <p>6) R6.3.3 appears to be redundant to and conflict with R4. These requirements are conceptually identical and the addition of R6.3.3 creates unnecessary confusion to include this annual 'vulnerability assessment' activity in R6. AZPS recommends moving this requirement to be a sub-R4 specific requirement added to the annual vulnerability assessment.</p> <p>7) R6.4.2 appears to not specify any log review or monitoring timeframe, as do many other logging/monitoring requirements in CIP-005-3 R3.2) and CIP-007-3 (R6). For example, CIP-005-3 R3.2 uses the phrase 'detect and alert' and includes a technical feasibility clause where alerting is not technically feasible that includes a 90-day review or assessment of the logs. CIP-007-3 R6 (and subsequent sub-requirements) include the term monitor, but also specific alerting and log review requirements. However, the term 'monitor' can have many interpretations, so AZPS is</p>

Voter	Entity	Segment	Vote	Comment
				<p>concerned about whether this term assumes a 24x7 human detect and response capability or other inherent log review requirements, especially when other Standards have additionally included these concepts where the term monitoring is used. AZPS recommends adding similar specificity for alerting or log review periods or clarifying what is meant by 'monitoring'.</p> <p>8) R6.5.4 utilizes the word 'agreement', but this word was changed to 'policy' in R6.5, which creates a potential conflict. AZPS recommends changing the word 'agreement' to the word 'policy' in R6.5.4.</p>
<p>Response: Thank you for your comments The SDT agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>The definition of “support or maintenance” has been created to define the uses of remote access for this requirement. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN.</p> <p>For 6.2, The SDT agrees with the intent of your comment but didn't include this into the requirement so as to not make the requirement too burdensome for some entities. AZPS may feel free to encrypt communications on its internet networks.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Gordon Rawlings	BC Transmission Corporation	1	Negative	BC Hydro agrees with the controls suggested around remote access but some clarification is required
Venkataramakrishnan Vinnakota	BC Hydro	2		R6 - This is pretty wide open. Suggest that specific requirements be put forth so entities know exactly what they need to comply with. Instead of

Voter	Entity	Segment	Vote	Comment
Pat G. Harrington	BC Hydro and Power Authority	3		<p>providing “examples” or “includes”, explicitly define those items that constitute support and maintenance.</p> <p>R6.4.2 – Recommends the use of SIEM technology to “alert” on access attempts by unauthorized parties. This automates the monitoring but would need clarification that this satisfies this requirement.</p> <p>R6.5 - Such a user agreement does make these users aware of their respective responsibilities in ensuring the security of the CCA in question. However, this is a weak control as an entity cannot influence direct control over how these entities implement security (i.e. Areva desktops) on their computer devices used to support entities CCAs. Does having such a signed agreement in place satisfy compliance? Can these agreements be entered into with organizations (i.e. Areva) as security policies are typically enforced uniformly throughout organizations?</p>
<p>Response: Thank you for your comments. Since the concepts of “support” or “maintenance” are so broad, it is not practical to provide a definitive list of what is or is not included within the concept. The Drafting Team believes the provided list of examples is sufficient.</p> <p>Requirements R6.3 and 6.4 have been modified in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Donald S. Watkins	Bonneville Power Administration	1	Negative	<p>Generally, BPA agrees with the objectives of the new proposed verbiage, however, it is too prescriptive and restrictive regarding remote access. Implementation decisions need be left to the entities. The current definition does not sufficiently allow for remote access to an ESP and the critical cyber assets contained there. This remote access is the typical method for gaining electronic access to critical cyber assets.</p> <p>1. Remote Access: Needs simplification - Recommended Change: “Remote access, for the purposes of this requirement and its sub-</p>
Rebecca Berdahl	Bonneville Power Administration	3		
Francis J. Halpin	Bonneville Power Administration	5		

Voter	Entity	Segment	Vote	Comment
Brenda S. Anderson	Bonneville Power Administration	6		<p>requirements, is interactive electronic access which is initiated from a point not located within any of the Responsible Entity's Electronic Security Perimeter(s). Remote access may be initiated from any cyber asset external to the Responsible Entities Electronic Security Perimeter(s)."</p> <p>2. Comment on R6.2 - Simplify and make this more technically correct - Recommended Change: "Implement remote access controls such that communications between cyber assets internal to the Electronic Security Perimeter(s), and systems used to perform remote access, are encrypted while operating on networks outside the Responsible Entity's control."</p>
<p>Response: Thank you for your comments. The SDT has attempted to balance the "what" issues with the "how" issues, and feels that the proposed standards (as modified in response to comments) provides a set of requirements, with sufficient flexibility in implementation.</p> <p>The SDT has made changes to both definitions, and believes that, with the changes, the definitions now meet the intent of BPA's suggestions.</p> <p>Requirement R6.2 has been updated based on this and other comments.</p>				
Tony Kroskey	Brazos Electric Power Cooperative, Inc.	1	Negative	<p>BEPC supports the development of this proposed Standard revision, but believes that the following items need to be improved or addressed:</p> <p>Add proxy system to R6. 2 as shown within parenthesis in the following: Implement the remote access system such that communications between the Cyber Asset performing remote access and the intermediate device (or proxy system) are encrypted while the communications traverse a network outside the control of the Responsible Entity.</p> <p>Add wording to R6.3.1 as shown within parenthesis in the following: R6.3.1. Restrict remote access to (users) authorized (by the) Responsible Entity (that include its) personnel and vendors (or others with a need for access).</p> <p>Replace the word "record" with the word "list" in R6.3.2 to replicate CIP-004-R4 language. Maintain a list of all individuals authorized for remote access and review the list in accordance with CIP-004-4 Requirement</p>

Voter	Entity	Segment	Vote	Comment
				<p>R4.</p> <p>Replace the word "create" with the word "creating" in R6.3.3. R6.3.3.</p> <p>Annually assess the implementation of the technical controls for remote access creating an action plan to remediate or mitigate any findings and document the execution status of that action plan.</p> <p>Add the word security to R6.5.2 as shown within parenthesis in the following: R6.5.2. Updating (security) patch levels for operating system and applications used for remote access</p> <p>The R6.5.4 requirement as written is problematic when dealing with vendor personnel.</p>
<p>Response: Thank you for your comments. The definitions have been modified in response to this and other comments. The parenthetical phrase in Requirement R6 has been deleted to remove ambiguity surrounding the status of the intermediary device.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Christopher L de Graffenried	Consolidated Edison Co. of New York	1	Affirmative	<p>[1] 6.3.3 – delete the word "technical" before "controls," delete the words "for remote access" before the word "create," add the words "any necessary" following the word "create," and move 6.3.3 under 6.4 as a new 6.4.3.</p> <p>[2] Change the wording in 6.4 from "technical controls" to "controls" to allow for procedural methods of implementing these controls.</p>
Peter T Yost	Consolidated Edison Co. of New York	3		
Wilket (Jack) Ng	Consolidated Edison Co. of New York	5		
Nickesha P Carrol	Consolidated Edison Co. of	6		

Voter	Entity	Segment	Vote	Comment
	New York			
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
John K Loftis	Dominion Virginia Power	1	Negative	<p>Dominion believes that dial-up connections should be specifically excluded from CIP-005-4-R6 or an option should be provided to allow for a technical feasibility exception (TFE) with an extended implementation timeframe. Dominion prefers that dial-up connections be excluded from CIP-005-4-R6 rather than allowing technical feasibility exceptions.</p> <p>There are two primary concerns that need to be addressed:</p> <p>First, CIP-005-4-R1.1 contradicts CIP005-4-R6.1 when such connections are established via remote access for maintenance and support. CIP-005-4-R1.1 allows access points to the ESP to include externally connected communication end points (for example, dial-up modems) terminating at any device within the ESP. This type of access point would be disallowed under CIP-005-4-R6.1 where access must be achieved via a proxy device for maintenance and support.</p> <p>Second, CIP-005-4-R6.2 requires encrypted communications between a remote device and an intermediate device. Certain systems that provide dial-up access and use non-routable protocols do not allow for an encrypted session to be established to the intermediate device after the initial connection has been made.</p>
Mike Garton	Dominion Resources, Inc.	5		
Michael F Gildea	Dominion Resources Services	3		
Louis S Slade	Dominion Resources, Inc.	6		
<p>Response: Thank you for your comments. The SDT believes that dial-up access meets the proposed definition of Remote Access, and should be protected using both multi-factor authentication and encryption. The definition has been updated to reflect this.</p> <p>Requirements R1.1 and R1.2 deal with establishing ESPs, not how to cross them or access Cyber Assets within the defined ESPs. The new R6 is focused on requirements placed on the Cyber Assets that initiate and manage interactive remote access.</p> <p>The technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p>				
Douglas E. Hils	Duke Energy Carolina	1	Negative	Duke Energy appreciates the work of the drafting team, but believes additional clarity is needed. Most importantly, R6.5 is unnecessary and would create significant compliance issues. Specific comments:

Voter	Entity	Segment	Vote	Comment
				<ul style="list-style-type: none"> • Second paragraph of R6 – Strike the word “monitoring” in order to avoid ambiguity with monitoring of equipment other than Cyber Assets. • Third paragraph of R6 – In order to emphasize that these are examples rather than an all-inclusive list, add the phrase “but are not limited to” after the phrase “Examples of support and maintenance activities include”. • Requirement 6.3.3 – This section addresses assessment of technical controls, and should be moved to R6.4 and renumbered R6.4.3. • Requirement 6.5 – This section should be deleted. Implementation of R6.1 through R6.4 establishes sufficient remote access controls, and R6.5 adds no value. R6.5 would create a significant compliance documentation problem that would drain resources without an attendant improvement in cyber security.
<p>Response: Thank you for your comments. The definitions have been modified based on this and other comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
David Batz	Edison Electric Institute	1	Abstain	EEI supports efforts to add additional controls for remote access to Electronic Security. We believe that the drafting team should carefully review feedback concerning the requirement for Third Party/Vendor remote access agreements.
<p>Response: Thank you for your comments. The definition of “interactive remote access” has been updated to address this issue.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which</p>				

Voter	Entity	Segment	Vote	Comment
addresses how the connection requirements can be met.				
George R. Bartlett	Entergy Corporation	1	Negative	As the CIP-005-3 red line document is currently worded there is no explicitly stated verbiage that dial-up will be considered as “remote access”. We recognize that there is statement in the Consideration of Comments on Initial Ballot issued that dial up will be included, however we believe it should be explicitly stated as such in the requirements to avoid any confusion.
Stanley M Jaskot	Entergy Corporation	5		
Terri F Benoit	Entergy Services, Inc.	6		
Response: Thank you for your comments. The definition of “interactive remote access” has been updated to address this issue.				
Robert Martinko	FirstEnergy Energy Delivery	1	Negative	<p>FirstEnergy (FE) appreciates the hard work and efforts of the project 2010-15 standard drafting team members who are performing revisions to the CIP-005-3 “Cyber Security — Electronic Security Perimeter(s)”. FirstEnergy recognizes that the team took great care to carefully review and respond to prior industry feedback, including those of FE, and implemented important changes based on that feedback. Many improvements have been made to the current draft of the version 4 standard which FE believes will ultimately drive industry support for the standard. However, at this time we are voting NEGATIVE based on the items summarized below. Thank you for considering our points of view on the proposed CIP-005-4 reliability standard. Our comments are based on the revised red-line standard dated 12-1-10 issued at the start of the ballot period, which superseded the 11-12-10 version provided during the ballot pool formation.</p> <p>1. FE recommends the removal of sub-requirement R6.5.4. FE supports the proposed revision to R6.5 to replace “agreement” with “policy”. However, sub-requirement R6.5.4 remains and indicates that for each remote user that a signed and dated acknowledgement of the remote access user “agreement” is required. FE recommends the removal of sub-requirement R6.5.4. This requirement presents an unnecessary and inappropriate administrative compliance burden which FE believes can be alleviated without sacrificing the controls desired by the team via R6.5.1 through R6.5.3. In sub-requirement R6.5.4 the word “all” implies each individual user and not simply each organizational entity being afforded remote access rights would need to sign and acknowledge the “remote access user agreement (policy)”. This presents a challenge since the individual FE staff provided with remote access rights are not typically employees having responsibility for the technical requirements</p>
Kevin Query	FirstEnergy Solutions	3		
Douglas Hohlbaugh	Ohio Edison Company	4		
Kenneth Dresner	FirstEnergy Solutions	5		
Mark S Travaglianti	FirstEnergy Solutions	6		

Voter	Entity	Segment	Vote	Comment
				<p>stated within R6.5.1 through R6.5.3 for the FE owned Cyber Devices they operate to initiate the remote access. It is the FE Infrastructure Technology staff that appropriately monitors, implements and maintains the controls described in sub-requirements R6.5.1 through R6.5.3 for such Cyber Devices. Therefore, it is not feasible or appropriate to maintain signed and dated acknowledgement by the users who may have no control over the technology utilized. Additionally, FE employees are not permitted access to Critical Cyber Assets via personal Cyber Assets and therefore this negates the agreement need for personal devices. The situation described above for FE staff also pertains to vendor company personnel having remote access from the vendor owned equipment. While FE agrees with the technical controls desired in R6.5.1 through R6.5.3 we believe that these statements are better reflected in a cyber policy and reinforced through the security awareness program required by CIP-004. Providing this detail in a company policy will drive better articulation of expectations of the organization's technical (IT) staff and remote access users (company employees and vendors). Therefore, we support the proposed change to R6.5 to replace "agreement" with "policy". However, we recommend that requirement R6.5.4 be removed as it is an unnecessary administrative burden and inappropriate as stated above. Furthermore, the awareness and training assessment requirements of CIP-004 should suffice as the acknowledgement once clear expectations associated with R6.5.1 through R6.5.3 are appropriately reflected in the overall company cyber policy. This acknowledgement is further supported by the personnel risk assessment of CIP-004 to provide a defense-in-depth approach for prudent approval of remote access privileges.</p> <p>2. FE proposes revision to the exemptions stated in the Applicability Section. The exemptions (Section 4.2) in the Applicability Section (Section 4) should be revised in regards to exemptions for nuclear generation facilities. Rather than complete removal of the existing version 3 exemption that reads: "Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission." it is suggested that this exemption be revised for consistency with the work of the project 2008-06 drafting team. Specifically, we propose that the exemptions be revised to read: 4.2.1 Facilities regulated by the Canadian Nuclear Safety Commission. 4.2.2 Cyber Assets associated with Cyber Security Plans submitted to and verified by the U. S. Nuclear Regulatory Commission pursuant to 10 C.F.R. Section 73.54. 4.2.3 Cyber Assets</p>

Voter	Entity	Segment	Vote	Comment
				<p>associated with communication networks and data communication links between discrete Electronic Security Perimeters. 4.2.4 Responsible Entities that, in compliance with Standard CIP-002-4, identify that they have no Critical Cyber Assets.</p> <p>3. Other minor edits proposed by FE</p> <p>A. In the Purpose section of the standard a reference to the version 3 CIP-009 standard remains and should be revised to reflect version 4 per changes being made in the 2008-06 project. In the last sentence please revise the text that reads “Standards CIP-002-4 through CIP-009-3” to read “Standards CIP-002-4 through CIP-009-4”</p> <p>B. In the Effective Date section of the standard insert the word “approval” after the reference to “BOT”.</p> <p>C. In regards to the explanatory text moved to the text box near the beginning of Requirement R6 we support this revision. However, it is unclear if the text box will remain in the final version of the standard or simply development guidance. If it remains, we offer the following observations. First, we recommend to strike “or contractors” from item 2 as it is redundant with and better placed in item 3. Second, the last sentence is missing text and should be updated if retained in the standard.</p>
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>The definitions have been modified based on this and other comments. Local definitions will remain as part of the standard.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p> <p>The effective date and purpose sections of the standard have been modified in response to this and other comments.</p>				

Voter	Entity	Segment	Vote	Comment
Ajay Garg	Hydro One Networks, Inc.	1	Negative	<p>1. This draft removed the exclusion of Canadian nuclear facilities. The same exclusion was recently reinstated in the proposed draft of CIP-002-4 after the comments received from Canadian entities. Canada has its own laws and regulations and all nuclear facilities within Canada are covered by them. The Canadian Nuclear Safety Commission (CNSC) has jurisdiction over the complete nuclear sites in Canada. We believe that a single regulator should have jurisdiction over the all assets and there should be no overlapping. As such the appropriate section should continue to exempt the nuclear facilities in Canada.</p> <p>2. We believe that requirements 6.3.1 and 6.3.2 should be removed. R6.3.1 and R6.3.2 could possibly present a double jeopardy with requirement R4 of CIP-004. This would result in non-compliance with two standards for a single infraction.</p>
David L Kiguel	Hydro One Networks, Inc.	3		
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Negative	<p>Major Issues for NPCC are as follows;</p> <p>The draft standard shows the removal of the Canadian nuclear exclusion, this should be reinserted and is a major issue for the Canadian Provinces.</p> <p>NPCC recommends removing R6.3.1 and R6.3.2 because of the double jeopardy(duplicity) with CIP-004 R4 which would result in non-compliance with two standards for a single infraction of the same access control issue.</p>
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
Donald E. Nelson	Commonwealth of Massachusetts	9	Negative	The draft standard shows the removal of the Canadian nuclear exclusion.

Voter	Entity	Segment	Vote	Comment
	Department of Public Utilities			<p>Recommend removing R6.3.1 and R6.3.2 because of the double jeopardy(duplicity) with CIP-004 R4 which would result in non-compliance with two standards for a single infraction of the same access control issue.</p> <p>Other less significant issues that should be addressed are;</p> <p>Recommend changing R6.4 from “technical controls” to “controls” to allow procedural controls</p> <p>Recommend removing R6.5 because 1) it is not readily auditable, 2) not enforceable by the Entity, 3) probably not technically feasible and in some aspects duplicated in R6.1</p> <p>Associated guidance document should have an explicit disclaimer that auditors cannot audit to this associated document. The guidance document is not and does not represent a change to any requirement so should not be used by an auditor.</p> <p>Request clarification of 6.2. What is the "Cyber Asset performing remote access"? The maintenance machine or the Cyber Asset being connected?</p>
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The associated guidance document is guidance only, not a set of requirements; therefore, the proposed requirements need to be added to Standard CIP-005 in order for them to become mandatory and enforceable. The disclaimer section of the associated guidance document states “[t]his supporting document may explain or facilitate implementation of reliability standard CIP-005-4 Requirement R6, but this supporting document does not contain mandatory requirements subject to compliance review.” The CMEP requires that auditors only audit</p>				

Voter	Entity	Segment	Vote	Comment
<p>to Requirements of approved standards.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p>				
David H. Boguslawski	Northeast Utilities	1	Negative	<p>1) The missing Canadian nuclear exclusion should be reinstated</p> <p>2) Associated guidance document should have an explicit disclaimer that auditors cannot audit to this associated document</p> <p>3) Request clarification of 6.2. What is the "Cyber Asset performing remote access"? The maintenance machine or the Cyber Asset being connected?</p> <p>4) Recommend removing R6.3.1 and R6.3.2 because of the double jeopardy with CIP-004 R4</p> <p>5) Recommend changing R6.4 from "technical controls" to "controls" to allow procedural controls</p> <p>6) Recommend removing R6.5 because: 1) not auditable, 2) not enforceable by the Entity, 3) probably not technically feasible and in some aspects duplicated R6.1</p>
<p>Response: Thank you for your comments. The SDT agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>The associated guidance document is guidance only, not a set of requirements; therefore, the proposed requirements need to be added to Standard CIP-005 in order for them to become mandatory and enforceable. The disclaimer section of the associated guidance document states "[t]his supporting document may explain or facilitate implementation of reliability standard CIP-005-4 Requirement R6, but this supporting document does not contain mandatory requirements subject to compliance review." The CMEP requires that auditors only audit to Requirements of approved standards.</p> <p>The term "performing" has been removed from Requirement 6.2.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual</p>				

Voter	Entity	Segment	Vote	Comment
<p>homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Roger C Zaklukiewicz		8	Negative	<p>Within Attachment A of the Standard an allowance is required upon which an RC could make a determination that a failure of a particular transmission facility would have no impact outside the local area and as such should not be subject to CIP Standard compliance requirements.</p> <p>The Canadian nuclear exclusion should be reinstated.</p> <p>There should be an explicit disclaimer that auditors would not be allowed to audit a facility for compliance with the associated guidance document.</p> <p>Require clarification of Section 6.2 - What is the "Cyber Asset Performing Remote Access".</p> <p>Need to remove R6.3.1 and R6.3.2 because of their double jeopardy with R4 of CIP-004.</p> <p>It will be virtually impossible to audit R6.5 therefore, it should be removed or revised.</p>
<p>Response: Thank you for your comments. The comment concerning "Attachment A" is apparently associated with Project 2008-06, not Project 2010-15.</p> <p>The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>The associated guidance document is guidance only, not a set of requirements; therefore, the proposed requirements need to be added to Standard CIP-005 in order for them to become mandatory and enforceable. The disclaimer section of the associated guidance document states "[t]his supporting document may explain or facilitate implementation of reliability standard CIP-005-4 Requirement R6, but this supporting document does not contain mandatory requirements subject to compliance review." The CMEP requires that auditors only audit to Requirements of approved standards.</p> <p>Requirement R6.2 has been updated based on this and other comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers</p>				

Voter	Entity	Segment	Vote	Comment
<p>Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Bernard Pelletier	Hydro-Quebec TransEnergie	1	Negative	<p>We recommend removing R6.3.1 and R6.3.2 because of the double jeopardy with CIP-004 R4.</p> <p>We also recommend removing R6.5 because 1) not auditable, 2) not enforceable by the Entity, 3) probably not technically feasible and in some aspects duplicated R6.1.</p> <p>Finally, the effective date of 6 months combined with R6 will have a big impact to the industries and can not be reached in a such short delay.</p>
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the "Version 4" standards recently approved by industry.</p>				
Saurabh Saksena	National Grid	1	Negative	<p>(i)The proposed standard has still not resolved the issues of double jeopardy and requests the drafting team to consider removing R2.3 and R2.4 and the corresponding text related to dial-up access to the new R6. This is necessary to avoid double jeopardy. Also, since "dial-up" is a form of remote access, it makes sense to move R2.3 and R2.4 to R6.</p> <p>(ii) National Grid also recommends a one-year time frame instead of six months to comply with the new requirement R6.</p>
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the "Version 4" standards recently approved by industry.</p>				

Voter	Entity	Segment	Vote	Comment
Randy MacDonald	New Brunswick Power Transmission Corporation	1	Negative	The draft standard shows the removal of the Canadian nuclear exclusion
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p>				
John C. Allen	Rochester Gas and Electric Corp.	1	Negative	<p>RG&E recommends removing R6.3.1 and R6.3.2 because of the double jeopardy (duplicity) with CIP-004 R4 which would result in non-compliance with two standards for a single infraction of the same access control issue.</p> <p>RG&E recommends removing R6.5 because it is not readily auditable, is not enforceable by the Entity, may not be technically feasible and in some aspects duplicated in R6.1.</p>
Kevin L Howes	Central Maine Power Company	1	Negative	<p>Central Maine Power recommends removing R6.3.1 and R6.3.2 because of the double jeopardy (duplicity) with CIP-004 R4 which would result in non-compliance with two standards for a single infraction of the same access control issue.</p> <p>Central Maine Power recommends removing R6.5 because it is not readily auditable, is not enforceable by the Entity, may not be not technically feasible and in some aspects duplicated in R6.1.</p>
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Ronald D. Schellberg	Idaho Power Company	1	Affirmative	Proposed changes to CIP-005 clarify requirements for remote access with the exception of R6.1.3. The language in R6.1.3 creates a requirement that will be difficult to measure compliance with and almost impossible for the Registered entity to develop a test or record it can be

Voter	Entity	Segment	Vote	Comment
				<p>assured meets each auditors personal thoughts on what constitutes a valid test.</p> <p>R6.1.3 should be reworded to “show that access controls implemented pursuant to Requirement R6.2 are configured to deny by default, access attempts by individuals not included in the record”.</p>
<p>Response: Thank you for your comments. The Drafting Team assumes you are referring to Requirement R6.3. Requirement R6.3 has been modified based on this and other comments.</p>				
Michael Holtsclaw	Indianapolis Power & Light Co.	1	Negative	<p>IPL's comments are as follows:</p> <p>1) R6 specifies that remote access can be initiated from “1) Cyber Assets owned by the Responsible Entity, 2) Cyber Assets owned by employees or contractors, and 3) Cyber Assets owned by vendors, contractors, or consultants.” However, R6.3.1 restricts remote access to “... authorized Responsible Entity personnel and vendors.” R6.3.1 needs to include contractors and consultants. R6 should be simplified so the three parts (1), 2), and 3)) be listed as one series. Finally, the term ownership disallows for those organizations and/or individuals that lease equipment. Proposed alternative language: “Remote access can be initiated from a Cyber Asset owned by or otherwise be under the control and responsibility of the Responsible Entity, employees, contractors, vendors, or consultants.”</p> <p>2) The categorization of the intermediate device or proxy system required to be implemented in R6.1 is vague. The stated intent of the SDT (EEI conference call 11/29/2010) to have this device not be an access point (R6.1) is not clear in the Requirement. R6.1 should explicitly state that the intermediate device or proxy system is not an access point in R1.1 when it communicates to cyber assets within the ESP through a defined access point. Proposed language to insert at the end of R6.1 is: The intermediate device or proxy system shall not be considered an access point or as a Cyber Asset used in the access control and/or monitoring of the Electronic Security Perimeter when remote traffic is retransmitted from the intermediate device or proxy system to a documented Electronic Security Perimeter access point to access a Cyber Asset within the Electronic Security Perimeter or the access point itself.</p>

Voter	Entity	Segment	Vote	Comment
				<p>3) R6.2 specifies encryption but does not specify a minimum level. An Entity could conceivably use something as simple as ROT-13, Caesar Cipher, or even better apply ROT-13 twice for double the strength. Recommend specifying FIPS standard or some other baseline.</p> <p>4) R6.4.2 specifies "... producing and monitoring of access logs of remote access." As there are no requirements to review the logs, the log monitoring is a very weak requirement. Additionally, the measure, M6, specifies "... documentation of the remote access controls as specified in Requirement R6" emphasis mine. As the logs are not performing a control function (no review), the logs are not a measure. Recommend replacing the word monitoring to reviewing.</p> <p>5) R6.5.4 is a significant increase in documentation tracking and is a departure from other CIP Requirements as no other CIP Requirement contains an equivalent to a user agreement. The sub requirements of R6.5 can be fulfilled by CIP-003 R1.1 and the use of technical controls. The original language may be suitable as a compensating measure/mitigation plan where it is not technically feasible. Suggested language: R6.5 Establish, implement, and document technical controls for Cyber Assets used to initiate remote access including the following, where technically feasible: R6.5.1 Updating anti-malware software and signatures R6.5.2 Updating security patches for operating system and installed applications R6.5.3 Prohibition of simultaneous network connections to devices other than those required for initiating and maintaining the remote access to a Electronic Security Perimeter and/or Cyber Assets contained within the Electronic Security Perimeter via the intermediate device or proxy system.</p> <p>6) R6 does very well in being general and not limiting in technology in which the Entity can perform the remote access until R6.5.3 where VPN configuration options are prohibited. Is it the intent that if remote access is performed via another method other than a VPN, the remote cyber asset can have active connections to assets in other networks or be "dual-homed"? R6.5.3 specifies the prohibition of "split-tunneling" and "dual-homed" workstations with out defining either term. Additionally, the use of the conjunction "and" indicates a logical operation of both conditions, thereby allowing an either or situation which is assumed is not the intention. If the VPN term is mandatory, a suggested wording would be "Prohibition of VPN/system configurations in which the remote</p>

Voter	Entity	Segment	Vote	Comment
				cyber asset can access the intermediate device or proxy system and any other non-ESP cyber asset simultaneously” which would additionally remove the possibility of “tri-homed” or system running multiple virtual interfaces on one network interface. Otherwise, please see the proposed R6.5.3 language in part 5 of our comment.
<p>Response: Thank you for your comments.</p> <p>The definitions have been modified in response to this and other comments.</p> <p>A section on encryption has been added to the associated guidance document.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Michael Moltane	International Transmission Company Holdings Corp	1	Affirmative	Although voting "Affirmative", ITC believes that the Access List required in R6.3.2 is already a requirement in CIP-004 and does not need to be duplicated here.
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
Michael Gammon	Kansas City Power & Light Co.	1	Negative	The proposed changes include the equipment and facilities of others which is outside the control or authority of an entity and impossible to enforce. In addition, the requirements for tracking logging out is unduly burdensome and does little to support security.
Charles Locke	Kansas City Power & Light Co.	3		
Jessica L Klinghoffer	Kansas City Power & Light Co.	6		

Voter	Entity	Segment	Vote	Comment
<p>Response: Thank you for your comments.</p> <p>The mandatory CIP Standards only make a distinction between Cyber Assets located within an ESP, and all other Cyber Assets. Since the standards do not place any other requirements on Cyber Assets not within an ESP, all Cyber Assets not located within an ESP are treated identically. The proposed new requirement is not intended to impose requirements on equipment and facilities outside the control or authority of the Responsible Entity.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments and in response to technical limitation arguments.</p>				
Martyn Turner	Lower Colorado River Authority	1	Affirmative	For R6 Remote access, for the purpose of CIP-005-4 Requirement R6 and its subrequirements, is non-supervised user interactive access by a person, used for monitoring, support, and maintenance, which originates from a Cyber Asset not located within any of the Responsible Entity's Electronic Security Perimeter(s). Or it should read: Remote access, for the purpose of CIP-005-4 Requirement R6 and its subrequirements, is user interactive (read and write) access by a person, used for monitoring, support, and maintenance, which originates from a Cyber Asset not located within any of the Responsible Entity's Electronic Security Perimeter(s).
<p>Response: Thank you for your comments. The Requirement is intended to apply to all access that meets the definition of "interactive remote access", whether supervised or not, and whether intended as read only or read-write. Note that access that is intended as "read only" can also be inadvertently "write" if not properly implemented and protected. The associated guidance document also presents a case study for access to data in a "read only" mode.</p>				
Joe D Petaski	Manitoba Hydro	1	Negative	<p>-R6: It is unclear whether R6 applies to all remote access, including "dial-up", or is limited only to remote access through a network. The draft guideline states "The guideline is intended to apply to the use of network-level remote access to CCAs across an ESP (i.e., access that uses a "routable protocol" rather than a "dial-up" connection)." This distinction needs to be clearly stated within the standard requirement.</p> <p>-R6: The requirement states that "... remote access can be initiated from: 1) Cyber Assets owned by the Responsible Entity 2) Cyber Assets owned by employees or contractors and 3) Cyber Assets owned by vendors, contractors, or consultants." This statement should be removed since remote access can be initiated from anywhere as long as it is compliant with R6 and the statement introduces a possible vulnerability if the Cyber Assets performing the remote access are not owned by the listed groups. If the statement's intent is that ONLY the listed Cyber Assets are allowed to initiate remote access, then the statement should</p>
Greg C. Parent	Manitoba Hydro	3		
Daniel Prowse	Manitoba Hydro	6		

Voter	Entity	Segment	Vote	Comment
				<p>be revised to clearly indicate that. In addition, if the statement is to remain contractors are listed in both 2) and 3) and should be removed from 2) for consistency.</p> <p>-R6.3: Suggested wording “Establish, implement and document procedural and technical controls for access authorization”</p> <p>-R6.3: Replace the phrase “Restrict remote access to Responsible Entity personnel and vendors” with “Restrict remote access to authorized individuals, in accordance with CIP-004 R4” to make it consistent with the rest of CIP-002 to CIP-009.</p> <p>-R6.3.3: Suggested wording “Annually assess the implementation of the technical controls for remote access. Create an action plan to remediate or mitigate any findings resulting from the annual assessment. Document the execution status of the action plan.” Presently as structured, R6.3.3 applies only to R6.3; it does not apply to all the technical controls in R6. If the intent was to perform an annual assessment for all the technical controls in R6, this sub-requirement would need to be at an R6.X level.</p> <p>-R6.4: Clarification required - do electronic access logs apply to Cyber Assets or to access points? i</p> <p>-R6.4: Suggested wording “Implement and document the processes for producing electronic access logs of remote access, which contain user identification, login time and logout or disconnect time of remote access, where technically feasible. Implement and document the processes for monitoring remote access, where technically feasible.”</p> <p>The rationale being that R6 shouldn't restrict us to the checking of logs as the only compliant method of monitoring remote access, which is not the best method of checking for unauthorized access anyway. By analogy on the physical security side, that would be like requiring us to monitor physical access logs to see if we have an intruder, instead of using motion detectors or security guard walk-about.</p> <p>-R6.5: This requirement needs clarification. An entity can document that its remote access user policy contains all these parts, but there is no requirement to actually implement any of the sub-requirements, although</p>

Voter	Entity	Segment	Vote	Comment
				<p>the language could imply implementation. As currently worded, for example, you need to have a remote access user policy that says it needs to be signed and dated, but there is no actual requirement for the user to sign and date the agreement (document but not implement). The explicit implementation language may have been excluded since it may be very difficult for a Responsible Entity to either implement or enforce these requirements on all remote access users. The current wording may lead to different audit expectations.</p> <p>-R6.5: Suggested wording “Acknowledgement of the remote access user agreement by all remote access users, including the date and some form of individual acknowledgement, such as physical or digital signature or other uniquely individual electronic acknowledgement”. This would make it possible for software such as SharePoint to manage the many remote access user agreements.</p> <p>-R6.5.3: Remove the use of the specific term “workstation” and replace it with the more generic and inclusive term “Cyber Asset”, which also provides consistency with the rest of the standard.</p> <p>- Changes in R6.5 from “remote access user agreement” to “remote access user policy” would require corporate policy change which may not be achievable 6 months after the NERC BOT approval.</p>
S N Fernando	Manitoba Hydro	5	Negative	<p>-R6: It is unclear whether R6 applies to all remote access, including “dial-up”, or is limited only to remote access through a network. The draft guideline states “The guideline is intended to apply to the use of network-level remote access to CCAs across an ESP (i.e., access that uses a “routable protocol” rather than a “dial-up” connection).” This distinction needs to be clearly stated within the standard requirement.</p> <p>-R6: The requirement states that “... remote access can be initiated from: 1) Cyber Assets owned by the Responsible Entity 2) Cyber Assets owned by employees or contractors and 3) Cyber Assets owned by vendors, contractors, or consultants.” This statement should be removed since remote access can be initiated from anywhere as long as it is compliant with R6 and the statement introduces a possible vulnerability if the Cyber Assets performing the remote access are not owned by the listed groups. If the statement’s intent is that ONLY the listed Cyber Assets are allowed to initiate remote access, then the statement should</p>

Voter	Entity	Segment	Vote	Comment
				<p>be revised to clearly indicate that. In addition, if the statement is to remain contractors are listed in both 2) and 3) and should be removed from 2) for consistency.</p> <p>-R6.3: Suggested wording “Establish, implement and document procedural and technical controls for access authorization”</p> <p>-R6.3: Replace the phrase “Restrict remote access to Responsible Entity personnel and vendors” with “Restrict remote access to authorized individuals, in accordance with CIP-004 R4” to make it consistent with the rest of CIP-002 to CIP-009.</p> <p>-R6.3.3: Suggested wording “Annually assess the implementation of the technical controls for remote access. Create an action plan to remediate or mitigate any findings resulting from the annual assessment. Document the execution status of the action plan.” Presently as structured, R6.3.3 applies only to R6.3; it does not apply to all the technical controls in R6. If the intent was to perform an annual assessment for all the technical controls in R6, this sub-requirement would need to be at an R6.X level.</p> <p>-R6.4: Clarification required - do electronic access logs apply to Cyber Assets or to access points? I</p> <p>-R6.4: Suggested wording “Implement and document the processes for producing electronic access logs of remote access, which contain user identification, login time and logout or disconnect time of remote access, where technically feasible. Implement and document the processes for monitoring remote access, where technically feasible.”</p> <p>The rationale being that R6 shouldn't restrict us to the checking of logs as the only compliant method of monitoring remote access, which is not the best method of checking for unauthorized access anyway. By analogy on the physical security side, that would be like requiring us to monitor physical access logs to see if we have an intruder, instead of using motion detectors or security guard walk-about.</p> <p>-R6.5: This requirement needs clarification. An entity can document that its remote access user policy contains all these parts, but there is no requirement to actually implement any of the sub-requirements, although</p>

Voter	Entity	Segment	Vote	Comment
				<p>the language could imply implementation. As currently worded, for example, you need to have a remote access user policy that says it needs to be signed and dated, but there is no actual requirement for the user to sign and date the agreement (document but not implement). The explicit implementation language may have been excluded since it may be very difficult for a Responsible Entity to either implement or enforce these requirements on all remote access users. The current wording may lead to different audit expectations.</p> <p>-R6.5: Suggested wording "Acknowledgement of the remote access user agreement by all remote access users, including the date and some form of individual acknowledgement, such as physical or digital signature or other uniquely individual electronic acknowledgement". This would make it possible for software such as SharePoint to manage the many remote access user agreements.</p> <p>-R6.5.3: Remove the use of the specific term "workstation" and replace it with the more generic and inclusive term "Cyber Asset", which also provides consistency with the rest of the standard.</p>
<p>Response: Thank you for your comments. The SDT believes that dial-up access meets the proposed definition of Remote Access and should be protected using both multi-factor authentication and encryption. The guidance document has also been updated to reflect this.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, in response to this and other comments, in response to this and other comments, and in response to technical limitation arguments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the "Version 4" standards recently approved by industry.</p> <p>The language in the definition of "interactive remote access" describing ownership of Cyber Assets has been modified.</p>				
Terry Harbour	MidAmerican Energy Co.	1	Negative	The proposed changes to CIP-005 prescribe "how" and not "what" should be accomplished. A couple prescriptive examples, installing jump servers or proxy systems and anti-virus on cyber assets used for remote access as mentioned. Such narrow prescriptions do not allow room for

Voter	Entity	Segment	Vote	Comment
				other alternate controls that would be equally or even more effective. Narrow prescriptions in a rapidly changing technology environment cause obsolesce faster the than standards revision process can update the requirements. For example, white listing in a control network environment is becoming more prevalent and is superior to anti-virus with signature updates. The CIP standards should focus on “what” is to be accomplished.
Dennis Kimm	MidAmerican Energy Co.	6	Negative	Please refer to MidAmerican Energy Company’s formal comments which include: “the proposed changes to CIP-005 prescribe “how.” A couple prescriptive examples, installing jump servers or proxy systems and anti-virus on cyber assets used for remote access. Such narrow prescriptions do not allow room for other alternate controls that would be equally or even more effective. Narrow prescriptions in a rapidly changing technology environment obsolesce technologically faster the than standards revision process can update the requirements. For example, white listing in a control network environment is becoming more prevalent and is superior to anti-virus with signature updates. Instead, improvements to CIP standards should be “what” is to be accomplished.”

Response: Thank you for your comments. This standard action is being developed in response to issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, not in response to any directive in FERC Order 706.

The associated guidance document is guidance only, not a set of requirements; therefore, the proposed requirements need to be added to Standard CIP-005 in order for them to become mandatory and enforceable. The disclaimer section of the associated guidance document states “[t]his supporting document may explain or facilitate implementation of reliability standard CIP-005-4 Requirement R6, but this supporting document does not contain mandatory requirements subject to compliance review.” The CMEP requires that auditors only audit to Requirements of approved standards.

Information provided by the US Government and included in the the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)”, published in March 2010, lead to concerns expressed over insecure remote access configurations; therefore, requirements concerning remote access are necessary. . The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.

The phrase “external interactive access into the Electronic Security Perimeter” in the former Requirement R2.4 only deals with the requirements placed on access through the ESP. The new Requirement R6 places additional requirements on the Cyber Asset initiating the interactive remote access, and places requirements on the communication and authentication mechanism in addition to the requirements for authorization in former Requirement R2.4.

The use of anti-virus with signatures is consistent with the language in CIP-007. Future standards development work by the Project 2008-06 SDT may change this concept, and if so, will make global changes to consistently address the issue.

The SDT has attempted to balance the “what” issues with the “how” issues, and feels that the proposed standards (as modified in response

Voter	Entity	Segment	Vote	Comment
to comments) provides a set of requirements, with sufficient flexibility in implementation.				
Douglas G Peterchuck	Omaha Public Power District	1	Negative	For 6.4.1, multifactor authentication has not been fully defined and what is the exact number of authentication factors required? Implementation time table is also an issue.
<p>Response: Thank you for your comments. The companion reference document “Secure Remote Access – Draft” provides an overview of multi-factor authentication. In addition, a footnote reference has been added to the standard.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
Michael T. Quinn	Oncor Electric Delivery	1	Negative	Through a proper implementation of the controls documented in CIP-005, sufficient protection is provided for the assets within an ESP. The definition of the ESP and protective measures identify the controls to access the environment and monitoring of activity within the environment. CIP-005-4 will add unnecessary paperwork and administrative overhead that does not increase reliability over the current standard. Requiring entities to implement additional systems for remote access will lead to unnecessary complexity and provide more points of failure. 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.
<p>Response: Thank you for your comments. Information provided by the US Government and included in the the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)”, published in March 2010, lead to concerns expressed over insecure remote access configurations; therefore, requirements concerning remote access are necessary. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p>				
John C. Collins	Platte River Power Authority	1	Negative	Urgent Action Revisions to CIP-005-3 Comments SDT Proposed: R6. Remote Access Controls —The Responsible Entity that allows remote access to Cyber Asset within its Electronic Security Perimeter(s) (or the Cyber Assets comprising the Electronic Security Perimeter’s access points) shall first implement the controls in the following subrequirements: PRPA Comments:
Carol Ballantine	Platte River Power Authority	6		
Terry L Baker	Platte River Power Authority	3		

Voter	Entity	Segment	Vote	Comment
Pete Ungerman	Platte River Power Authority	5		<p>As proposed Requirement R6 pertains solely to maintenance activities performed remotely. Understanding the desire to scope the additional requirement, PRPA feels that these controls should be implemented on all remote interactive connections originating from outside the ESP regardless of their function. This will remove the confusion of having to define remote maintenance access and support and maintenance while increasing security. Using “Remote Access Controls” implies the implementation of access controls for all remote access types. In addition there is a potential for overlap with existing dial-up access controls already covered in Requirement CIP-005-3 R2.</p> <p>It would be helpful if the drafting team added two new definitions to the NERC glossary: Remote Access, Dial-up Access. Remote Access would cover temporary external interactive ESP access using routable protocols while Dial-up Access would cover temporary external interactive ESP access using modems.</p> <p>PRPA suggests the following language. PRPA proposed language: R6. Remote Access Controls —The Responsible Entity shall implement the following controls for interactive remote access to Cyber Assets located within an Electronic Security Perimeter(s) or to the Electronic Security Perimeter access point Cyber Assets:</p> <p>SDT Proposed: R6.1. Implement an intermediate device or proxy system such that the Cyber Asset performing remote access does not have direct network access to Cyber Asset(s) within the Electronic Security Perimeter.</p> <p>PRPA Comments: PRPA has no comments for R6.1 but suggests the following language. PRPA proposed language: R6.1. Implement an intermediate device or proxy system such that the remote Cyber Asset does not have direct network access to the Cyber Asset(s) located within the Electronic Security Perimeter.</p> <p>SDT Proposed: R6.2. Implement the remote access system such that communications between the Cyber Asset performing remote access and the intermediate device are encrypted while the communications traverse a network outside the control of the Responsible Entity.</p>

Voter	Entity	Segment	Vote	Comment
				<p>PRPA Comments: An encryption tunnel may also terminate at an Electronic Security Perimeter access point Cyber Asset in addition to the intermediate device. Networks inside the control of the Responsible Entity aren't necessarily secure. CIP communications should be secured when they leave an ESP access point. PRPA suggests the following language. PRPA proposed language:</p> <p style="padding-left: 40px;">R6.2. Implement the remote access such that communications between the remote Cyber Asset and the intermediate device or Electronic Security Perimeter access point Cyber Asset are encrypted while traversing networks outside the Electronic Security Perimeter access point(s).</p> <p>SDT Proposed: R6.3. Establish, implement, and document procedural controls for access authorization of remote access to the Electronic Security Perimeter that include the following: R6.3.1. Restrict remote access to authorized Responsible Entity personnel and vendors. R6.3.2. Maintain a record of all individuals authorized for remote access and review these records in accordance with CIP-004-4 Requirement R4. R6.3.3. Annually assess the implementation of the technical controls for remote access create an action plan to remediate or mitigate any findings and document the execution status of that action plan. PRPA Comments: Entities have established, implemented, and documented procedural controls for access to the ESP.</p> <p>PRPA believes that R6.3, R6.3.1, and R6.3.2 have already been covered in CIP-005 R2 and that CIP-005 R2 applies equally to remote access through the ESP. The proposed R6.3.3 should be moved under the proposed R6.4 as both deal with technical controls. PRPA proposed language:</p> <p style="padding-left: 40px;">R6.3, R6.3.1, R6.3.2 should be removed. R6.3.3 should be moved under R6.4.</p> <p>SDT Proposed: R6.4. Establish, implement, and document technical controls to prevent unauthorized individuals from establishing remote access. R6.4.1. Require the use of multifactor authentication for all remote access. R6.4.2. Implement and document the processes for producing and monitoring electronic access logs of remote access, which contain user identification, login time and logout or disconnect time of remote access, where technically feasible.</p> <p>PRPA Comments: PRPA has no comments for R6.4 but suggests the</p>

Voter	Entity	Segment	Vote	Comment
				<p>following language which included the addition of 6.3.3. PRPA proposed language:</p> <p>R6.4. (R6.3) Establish, implement, and document technical controls to prevent unauthorized individuals from establishing remote access.</p> <p>R6.4.1. (R6.3.1) Require the use of multifactor authentication for all remote access.</p> <p>R6.4.2. (R6.3.2) Implement and document the processes for producing and monitoring electronic access logs of remote access, which contain user identification, login time and logout or disconnect time of remote access, where technically feasible.</p> <p>R6.4.3. (R6.3.3) Annually assess the implementation of the technical controls for remote access and create an action plan to remediate or mitigate any findings and document the execution status of that action plan.</p> <p>SDT Proposed: R6.5. Document a remote access user policy regarding Cyber Assets used to initiate remote access that requires: R6.5.1. Updating anti-malware software and signatures R6.5.2. Updating patch levels for operating system and applications used for remote access R6.5.3. Prohibition of VPN “split-tunneling” and “dual-homed” workstations which can concurrently access multiple networks R6.5.4. Signed and dated acknowledgement of the remote access user agreement by all remote access users.</p> <p>PRPA Comments: PRPA has no comments for R6.5 but suggests the following language. PRPA proposed language:</p> <p>R6.5. (R6.4) Document a remote access user policy and associated agreement requiring remote access users:</p> <p>R6.5.1. (R6.4.1) Update anti-malware software and signatures</p> <p>R6.5.2. (R6.4.2) Update patch levels for operating system and applications used for remote access</p> <p>R6.5.3. (R6.4.3) Disable VPN “split-tunneling” and “dual-homed” workstations which can concurrently access multiple networks</p> <p>R6.5.4. (R6.4.4) Sign and date an acknowledgement of the remote access user agreement.</p>

Voter	Entity	Segment	Vote	Comment
<p>Response: Thank you for your comments.</p> <p>The definition of “support or maintenance” has been created to define the uses of remote access for this requirement. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN.</p> <p>The SDT believes that dial-up access meets the proposed definition of Remote Access. Additional definitions are therefore not necessary.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Sammy Roberts	Progress Energy Carolinas	1	Negative	<p>Although we are casting a negative ballot on the Expedited Revisions to CIP-005-3, Progress Energy believes the current draft addresses the purpose and intent of the SAR, and provides requirements for implementing remote access that are both secure and achievable.</p> <p>Our ballot is negative because in Requirement R6.1 the purpose of the “intermediate device or proxy system” is not clearly stated, nor is its position relative to the ESP clearly stated.</p> <p>Also, R6.5.4 is impractical as written, as it needs a clause to allow an organization (e.g. a vendor technical support organization, or even the responsible entity itself) to attest to the agreement (policy) on behalf of employees using computers owned by the organization. We will provide input directly to the drafting team on how to remove these deficiencies.</p>
Sam Waters	Progress Energy Carolinas	3		
John T Sturgeon	Progress Energy	6		
Wayne Lewis	Progress Energy Carolinas	5		
<p>Response: Thank you for your comments.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers</p>				

Voter	Entity	Segment	Vote	Comment
<p>Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Pawel Krupa	Seattle City Light	1	Affirmative	R6.5 would require a signed user agreement for remote access users.
Dana Wheelock	Seattle City Light	3		The effectiveness and value of stipulating R6.5.1 – R6.5.2 is questionable. Many users do not have the ability (rights) to manage anti-virus signatures and patch levels on their company-issued systems.
Hao Li	Seattle City Light	4		Users cannot and should not agree to a policy that requires adherence to requirements that are beyond their control and requirements that they may not have visibility into. Numerous remote access technologies exist that perform technical enforcement of end point health status (the remote access server performs a health assessment on the originating end point before the remote session is allowed.) The standard should allow for such technologies in lieu of a prescriptive policy statement that cannot effectively and consistently accomplish the intended result of this requirement.
Michael J. Haynes	Seattle City Light	5		R6.5.3 prohibits remote access connections with split tunneling. This requirement would make sense and add value to remote access sessions where direct network access is available to critical cyber assets. The requirement for a proxy system to broker all remote sessions negates the need for split tunneling restrictions. This requirement also limits the selection of remote access technologies (such as some SSL remote access tools.) Remote access technologies rapidly evolve and requiring a technical control that is already becoming outdated will limit the ability to adopt emerging technologies (that will likely offer enhanced security.) One year will provide a better opportunity to design, procure, implement, test, and train for what will likely be a major infrastructure change for many utilities with complex environments.
<p>Response: Thank you for your comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				

Voter	Entity	Segment	Vote	Comment
Larry Akens	Tennessee Valley Authority	1	Negative	<p>Tennessee Valley Authority (TVA) appreciates the opportunity to comment on this CIP-002-4 draft. We fully support the standards development process and all the hard work and commitment by the drafting team members. For this draft, we have the following concerns which moved us to cast a Negative vote.</p> <p>R6 - support and maintenance is defined, but monitoring isn't. Recommend removing the word monitoring.</p> <p>R6 - Once access to a discrete ESP has been accomplished, can we then navigate to / access our other ESPs without being bound to R6 protections, or is access to each discrete ESP subject to the R6 protections?</p> <p>R6.1 - it isn't clear if the "intermediate device or proxy system" is the VPN or the jump server. What is the definition of "intermediate devices"? Need additional clarification to know what is included, and to clarify where in the network topology device would reside. What is network path to the proxy device? Is it through existing access control and monitoring devices (firewalls, etc) or does proxy reside outside ESP access point (in front of the firewall, for example)?</p> <p>R6.2 - the term "remote access system" isn't clear. What makes up a remote access system?</p> <p>R6.3 - says "...remote access to the ESP," should this be "into the ESP?"</p> <p>R6.4 - says "...can establish remote access." Without clarity of "remote access system" it is unclear if this is to take place at the VPN server outside the ESP or the jump server located within the ESP. It is recommended that it is to the jump server located within the ESP.</p> <p>R6.4.1 - Is "remote access" referring to the VPN server outside the ESP or the jump server located within the ESP? It is recommended that it is to the jump server located within the ESP.</p> <p>R6.4.2 - States "...access logs of remote access...", is this referring to the VPN server outside the ESP or the jump server located within the ESP?</p>
Ian S Grant	Tennessee Valley Authority	3		
George T. Ballew	Tennessee Valley Authority	5		
Marjorie S. Parsons	Tennessee Valley Authority	6		

Voter	Entity	Segment	Vote	Comment
				<p>It is recommended that it is to the jump server located within the ESP.</p> <p>R6.5 - This requirement should not be for cyber assets owned or operated by the Responsible Entity.</p> <p>R6.5.2 - This should include all operating systems and applications on the remote system, not just applications used for remote access.</p>
<p>Response: Thank you for your comments.</p> <p>The term “monitoring” has been removed from the definition for “interactive remote access”. The definition of “interactive remote access” specifically indicates that the access must originate from outside an ESP in order to be covered by this requirement. If access is initiated from within an ESP, it does not meet the definition of “interactive remote access” and Requirement R6 would not apply.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>The word “system” has been removed from Requirement 6.2.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
John Tolo	Tucson Electric Power Co.	1	Negative	<p>The proposed changes do not contribute substantively to the current version of CIP-005. Reviewing the proposed standard also indicated that the proposed revisions should indicate “what” is required rather than “how” to comply.</p> <p>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.</p> <p>SMEs reviewing the proposed standard also indicated that the proposed</p>

Voter	Entity	Segment	Vote	Comment
				<p>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.</p> <p>Review also indicates that there is no definition of “remote access” in the proposed standard. There is a lack of definition for intermediate system. The standard needs to be more prescriptive.</p> <p>CIP-005-3 contains a cyclical nature of the intermediate system. The proposed language appears to mandate such a system be in place for all cyber assets, yet the device itself is made to be a cyber asset. This didn't pass logical muster to us and creates a somewhat paradoxical situation.</p>
<p>Response: Thank you for your comments. The SDT has attempted to balance the “what” issues with the “how” issues, and feels that the proposed standards (as modified in response to comments) provides a set of requirements, with sufficient flexibility in implementation.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>Requirements R6.3 and 6.4 have been modified in response to this and other comments.</p> <p>Note that the intermediate device is a “Cyber Asset”, but not necessarily a “Critical Cyber Asset”.</p>				
Jonathan Appelbaum	United Illuminating Co.	1	Negative	<p>See UI Comments for full comments.</p> <p>UI main concern is UI does not agree with R6.5. Utilizing documentation to replace a technical control is not a strong security approach. There are several difficulties with R6.5 for both a Company employee and a support vendor.</p> <p>Requiring a remote access user, whether a company employee or a vendor support group, to sign a document will not provide any increase level of security or layered defense to the ESP.</p> <p>Second, an employee utilizing a Company supported computer can not honestly state that anti-virus updates and patching will occur since they are not in control of the process. Forcing users to sign agreements that they may neither understand nor control will not enhance reliability and introduces a level of dishonesty into the compliance process.</p>

Voter	Entity	Segment	Vote	Comment
<p>Response: Thank you for your comments. Please refer to our responses in the comment document.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Brandy A Dunn	Western Area Power Administration	1	Negative	<p>1. Standard CIP-005-4 R2 Electronic Access Controls fails to define the term "Electronic Access". This term is sufficiently ambiguous that NERC thought it was necessary to issue a Compliance Action Notice (CAN) on October 25, 2010 which clarified the term for the purposes of CIP-004-2 R4.2 and CIP-004-3 R4.2. The language in the CAN is very clear and should be incorporated directly into Standard CIP-005-4 R2.</p> <p>2. The CAN also clarifies the term "Remote Electronic Access". The definition in the CAN is at odds with the proposed definition of "Remote Access" in Standard CIP-005-4 R6. This is a problem for several reasons:</p> <ul style="list-style-type: none"> a. Having multiple definitions in various NERC documents will lead to confusion and make compliance more difficult. b. The proposed definition in Standard CIP-005-4 R6 is actually a subset of the definition contained in the CAN because it deals only with the portion of remote access used for monitoring, support, and maintenance. This leaves wide open the question as to what remote access controls are required for remote access which is not used for or monitoring, support, and maintenance. NERC should not approve the standard until it clearly addresses the remote access controls required for ALL types of remote access. Failure to do this will lead to confusion and make compliance more difficult.
<p>Response: Thank you for your comments. The subject of CAN-0005 was access used to control systems; the subject of the revisions to CIP-005 is access for the purpose of support or maintenance of systems. Work being done by the Project 2008-06 SDT will consider addressing all aspects of remote access.</p>				
Mark B Thompson	Alberta Electric System Operator	2	Negative	<p>The definitions and amendments proposed have clarified some of the concerns, but may have created additional complications in the process. NERC has created a new requirement R6 that creates three new terms - monitor, support, and maintain – but has only defined support and maintain.</p>

Voter	Entity	Segment	Vote	Comment
				<p>The AESO is requesting a definition for the term monitor.</p> <p>Additionally the new terms do not address a requirement for “business use and functions.” For example, in a case where system controllers must use a remote access device to manage the EMS – it would appear this job function is not addressed by any of the new terms.</p> <p>The AESO feels R6.1 does not clearly indicate if the intermediate device should reside inside or outside the ESP. R6.1 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 where this intermediate device should reside - is it inside or outside the ESP? If it is inside the ESP, then the intermediate device itself becomes a Cyber Asset, and according to R6.1 remote access to this device will also require an intermediate device. This potentially causes an infinite loop. If it is outside the ESP, then this intermediate device is not afforded the protections in R1.4 and R1.5 which is not the intent for systems providing (remote) access control. We believe the drafting team’s intention is for the intermediate device to reside inside the ESP, and therefore the AESO is requesting NERC to amend the wording for R6.1 to clarify their intent.</p> <p>We request that the SDT clarify the intent of encryption in requirement R6.2, and to consider further defining the term encryption. There are many forms of encryption, some stronger than others. It is unclear what, if any, minimum level of encryption would suffice.</p> <p>The AESO believes R6.3.3 should read “Annually assess the implementation of the procedural controls for remote access, create...”, and that a new requirement R6.4.3 should be created the same as the proposed R6.3.3 (i.e., to “Annually assess the implementation of the technical controls...”</p> <p>We believe R6.5 includes requirements that are difficult to implement. It is unclear which party, employer or employee, would bear the costs and the risks with these requirements. The result would be a requirement that would be difficult to control, and more difficult to enforce. The question is</p>

Voter	Entity	Segment	Vote	Comment
				further blurred when contractors and vendors are considered. If the SDT decides to keep R6.5, then R6.5.4 should include a provision for annual acknowledgement.
<p>Response: Thank you for your comments.</p> <p>The term “monitoring” has been removed from the definition for “interactive remote access”.</p> <p>The function referenced in your comment concerning “business use and functions” is addressed in CAN-0005. The revisions to CIP-005 address support or maintenance access.</p> <p>The definition of “interactive remote access” specifically indicates that the access must originate from outside an ESP in order to be covered by this requirement.</p> <p>A section on encryption has been added to the associated guidance document.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Kim Warren	Independent Electricity System Operator	2	Negative	The exemption clause pertaining to facilities regulated by the Canadian Nuclear Safety Commission (Section 4.2.1) must be reinstated to keep CIP-005-4 “in sync” with the changes occurring in CIP-002-4. Our detailed comments were submitted on the comments form for this posting.
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p>				
Kathleen Goodman	ISO New England, Inc.	2	Negative	<p>Overall, ISO New England supports the direction of the current standards development, with the exception of the comments submitted through normal process:</p> <p>In R6.2 the "Cyber Asset performing remote access" must be clarified. Is it the maintenance machine, or the Cyber Asset being connected?</p> <p>Remove R6.3.1 and R6.3.2 because of the double jeopardy with CIP-004 R4.</p>

Voter	Entity	Segment	Vote	Comment
				<p>Change the wording in R6.4 from “technical controls” to “controls” to allow for procedural controls.</p> <p>R6.5 should be removed because it is not auditable, not enforceable by the Entity, and most likely not technically feasible, and in some aspects duplicates R6.1.</p>
<p>Response: Thank you for your comments.</p> <p>The term “performing” has been removed from Requirement 6.2.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	<p>We would like to thank the drafting team for the many improvements they made to this version of the draft standard. The draft standard has improved greatly. However, we do believe there are some additional changes that are necessary before this standard is finalized. We offer the following comments on the need for additional changes.</p> <ol style="list-style-type: none"> 1. R6.2 references implementing a remote access system. Is this intended to reference the intermediate device or proxy system identified in R6.1? If so, consistent language should be used between these two sub-requirements. 2. We thank the drafting team for defining remote access. We are concerned about how the definition is implemented. Our understanding is that the text boxes get removed from the final version of the standard. If this is the case, then the definition should be added to the NERC Glossary of Terms. If the text box remains in the final version, then this implementation is satisfactory. 3. R6.3.2 is duplicative to CIP-004-3 R4. If the standards drafting team

Voter	Entity	Segment	Vote	Comment
				<p>believes that a specific remote access list is necessary, CIP-004-3 R4 and its sub-requirements should be modified rather than adding a new requirement to CIP-005-4.</p> <p>4. R6.3.2 references CIP-004-4. Version 4 of CIP-004 does not exist and is not proposed in this standards action.</p> <p>5. R6.3.3 is ambiguous and confusing. What is the purpose? It references technical controls. Is the purpose to assess the procedural controls identified in R6.3 or the technical controls identified in R6.4? If the purpose is to assess the procedural controls in R6.3, then that same term should be used rather than technical controls. If the purpose is to address the technical controls in R6.4, then this sub-requirement should be moved there. If the purpose is essentially to assess how good your procedural controls are, then R6.3.3 should be struck as it has no place in the standard. Standards should define what is required and not how to ensure your company complies with other requirements.</p> <p>6. R6.2.3: This requirement is duplicative to other system logging and access point requirements in 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. Isn't it industry standard to identify the IP address from which the logging is occurring? If so, there is no need for separate logging for remote access.</p> <p>7. R6.5 and R6.5.4 are administrative requirements and should be struck. There is no need to have an agreement between the user and responsibility entity. The remote access user may not even have the ability to ensure the operating system has updated patches, etc. as this is likely handled from a centralized department within the company and is often "pushed" to the laptops. Thus, how can the user agree to maintain their operating system when they have no control over it? This is a Catch-22.</p> <p>8. Any remote access policy issues or necessary acknowledgements can and should be handled through cyber security policy requirements in CIP-003-3 and training and awareness requirements in CIP-004-3.</p> <p>9. It is not clear how R.6.5.1 differs from CIP-007-3 R4 and its sub-</p>

Voter	Entity	Segment	Vote	Comment
				<p>requirements. Is it not duplicative?</p> <p>10. Is it not clear how R6.5.2 differs from CIP-007-3 R and its sub-requirements? Is it not duplicative?</p> <p>11. 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. We submitted this comment in the previous ballot and the drafting team essentially responded that it is limiting itself to technical changes to the standard. Based on the paragraph that begins with “Going forward, however ‘components’ ... with only the integer value of the requirement”, we do not believe the drafting team has the option to deviate from the filing.</p>
<p>Response: Thank you for your comments.</p> <p>Requirements R6.1 and R6.2 have been rewritten in response to this and other comments. The term “system” has been removed from Requirement R6.2. The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment. Local definitions will remain as part of the standard.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, in response to this and other comments, and in response to technical limitation arguments.</p> <p>Requirement R6.2 has been updated based on this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>This standards action has followed the requirement numbering convention of other requirements in CIP-005 (and the other “Version 4” CIP Standards).</p>				
Tom Bowe	PJM Interconnection, L.L.C.	2	Negative	R6 Remote Access Control – Needs clarification on “User interactive access by a person”. Does this means the person has to logically login to the cyber asset with his/her credentials? Or if the user logs in to an application outside of the ESP and the application connects to cyber assets (user is not using his/her credentials), would that be consider an interactive access “by a person”?

Voter	Entity	Segment	Vote	Comment
				<p>R6.2 – This is specific for communication traversing a network outside the Responsible Entity’s control; what happens if the Responsible Entity owns the network? Would encryption be required?</p> <p>R6.3.3 - Consider striking this paragraph.</p> <p>R6.3 addresses the implementation of procedural controls, while requirement R6.3.3 addresses the assessment of “technical controls”. Also, it is not clear what findings are considered in determining a violation.</p> <p>R6.5 – It should be specific to vendor access and not the Responsible Entity’s own systems.</p> <p>R6.5.4 – What constitute a signature, would that be a physical signature or an electronic signature suffice?</p>
<p>Response: Thank you for your comments. Requirement R6 applies to interactive remote access for the purpose of support or maintenance. It does not apply to application access (unless that application is a support or maintenance application meeting the definition of “support or maintenance”).</p> <p>Requirement R6.2 has been modified to indicated when encryption is required.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Bob Reeping	Allegheny Power	3	Negative	Allegheny Power is not voting in favor of this standard due the following issue. This standard should not duplicate requirements from other standards, but rather reference those requirements.
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				

Voter	Entity	Segment	Vote	Comment
Bruce Krawczyk	ComEd	3	Negative	<p>CIP-005-4, A-5 Effective Date.</p> <ul style="list-style-type: none"> •Proposed compliance date for changes to current CIP-005-3 (nine (9) months from Regulatory Approval (FERC) to effective date, six (6) months from effective date to compliance) may be too short for changes to be completed and tested for system reliability. This interval could impact the current ComEd SCADA Refresh Project, occurring in the final stages the project, which did not include these requirements in the project Statement of Work. There could be a risk to timely project completion or risk of inability to make the new system compliant in the time available. <p>CIP-005-4, R6 Remote Access Controls.</p> <ul style="list-style-type: none"> •These requirements would impact each operating company (ComEd, GenCo, PECO, PowerTeam) in different ways, but would apply to all OPCO's vendor and/or support access. •All SCADA systems would require evaluation and planning for compliant remote access solutions, since all systems appear to have some type of remote access, by internal staff, vendor support staff or both. CIP-005-4, R6.1 Proxy Server/Jump Host. •Clarification needed on the status of the proxy server required by R6-1. Is it an Access Control and Monitoring Asset (AMA) or is it not in scope of NERC requirements. It sits outside the Electronic Security Perimeter (ESP), but it intimately connected to access to ESP. What NERC reporting and control requirements would apply to this class of device? CIP-005-4, R6.2 Encrypted Communications •The requirement speaks of a requirement to encrypt communications outside the control of the responsible entity. Exelon has made the interpretation of this requirement that since BSC Infrastructure and Operations (I&O) Networking groups support all networks within the Exelon enterprise, that BSC IT I&O performs as a proxy for each of the OPCO's who are the responsible entities for Exelon. We are requesting clarification of this requirement for companies with more than one responsible entity within the corporate structure. CIP-005-4, R6-3

Voter	Entity	Segment	Vote	Comment
				<p>Authorization and Record Keeping.</p> <ul style="list-style-type: none"> •This requirement should address the procedural controls needed to access or utilize the intermediate device or proxy system instead of reiterating the existing CIP-005 R2 requirements for access through the Electronic Security Perimeter. As currently defined these intermediate devices or proxy systems are outside the scope of the other cyber security requirements in CIP-002 through CIP-009 since they must be located outside of the Electronic Security Perimeter. Any additional requirements for access through the Electronic Security Perimeter should instead be included in CIP-005 R2 or R3. •Recommended wording would be “Establish, implement and document procedural controls for the access authorization of remote access to the intermediate device or proxy system required in CIP-005-4 R6.1. •R6.3.3 should be moved to R6.4.3, since it is a technical control, not a procedural control. CIP-005-4, R6-4 Technical Controls for Access. •This requirement should address the technical controls needed to access or utilize the intermediate device or proxy system. Recommended wording would be: •Establish, implement and document technical controls to ensure that only authorized individuals can establish remote access to the intermediate device or proxy system required in CIP-005-4 R6.1” •R6.4.1 should be clarified to exactly which access requires multi-factor authentication: The ESP or the proxy/jump server? <p>CIP-005-4, R6-5 Remote Access User Agreement</p> <ul style="list-style-type: none"> •This requirement should be eliminated. This is only additional administrative documentation that does not ensure the remote cyber devices are implementing the items referenced. Ensuring remote end users understand the implication of these identified risks would be better addressed by including these topics in the annual training required in CIP-004 R2.2. Typical end users will also not know or be able to control

Voter	Entity	Segment	Vote	Comment
				if their corporately provided cyber devices are truly configured or maintained as referenced.
<p>Response: Thank you for your comments.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p> <p>Requirement R6.2 has been modified to indicated when encryption is required.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Lee Schuster	Florida Power Corporation	3	Negative	<p>Although we are casting a negative ballot on the Expedited Revisions to CIP-005-3, Progress Energy believes the current draft addresses the purpose and intent of the SAR, and provides requirements for implementing remote access that are both secure and achievable.</p> <p>Our ballot is negative because in Requirement R6.1 the purpose of the “intermediate device or proxy system” is not clearly stated, nor is its position relative to the ESP clearly stated.</p> <p>Also, R6.5.4 is impractical as written, as it needs a clause to allow an organization (e.g. a vendor technical support organization, or even the responsible entity itself) to attest to the agreement (policy) on behalf of employees using computers owned by the organization. We will provide input directly to the drafting team on how to remove these deficiencies.</p>
<p>Response: Thank you for your comments.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p>				

Voter	Entity	Segment	Vote	Comment
<p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Darl Shimko	Madison Gas and Electric Co.	3	Affirmative	<p>Although we are voting in the affirmative, we believe the standard should be further revised:</p> <p>1) We do not agree with the six month implementation plan for R6. It should be a one year time frame to give entities the ability to fully review and implement controls as required to R6.</p> <p>2) Additional clarity is needed to delineate which access control systems fall under the scope of CIP standards. For example, when remote access to a Cyber Asset is accomplished from the Internet to a corporate network via a VPN and then into the ESP according to the requirements of CIP005, is the VPN and its access control components a CIP access control system? If it is, where does the scope of CIP end? Is the PC/Laptop used for remote access a CCA or an access control system?</p> <p>3) Clarity is also needed to understand the label placed on the proxy system discussed in R6.1. Is the proxy the access point, an access control device or a critical cyber asset?</p> <p>4) The standard covers remote access "used for monitoring, support and maintenance". Why is this distinction made? What controls are suppose to be used for remote access for purposes of CA control?</p>
Joseph G. DePoorter	Madison Gas and Electric Co.	4		
Steven Schultz	Madison Gas and Electric Co.	5		
Jeffrey M Keebler	Madison Gas and Electric Co.	6		
<p>Response: Thank you for your comments.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p> <p>A new definition for “intermediate device” has been added the CIP-005-4 which addresses this issue. Additionally, the associated guidance document addresses a number of implementations, which provides further guidance.</p> <p>Remote access for the purpose of Critical Asset control is covered in CAN-0005.</p>				
John S Bos	Muscatine Power & Water	3	Affirmative	MP&W appreciates the work done by the STD; however, does not agree with the proposed implementation language (six months to comply with

Voter	Entity	Segment	Vote	Comment
				<p>the new Requirement R6 after the standard becomes effective). If a Registered Entity has remote Substations designated as Critical Assets, 6 months does not provide sufficient time for research into technologies, re-design of the Substation Automation Networks, or the installation and testing. If this were only applied to EMS/SCADA systems at control centers, 6 months would be adequate in most cases. Conversely, when Registered Entities have lengthy travel distances to and from these remote Substations, and that same travel is again required for troubleshooting, 6 months does not provide a realistic implementation period for the new requirements placed on entities in R6 (installation of proxy servers, remote access systems, and new access controls). MP&W recommends 18 months for implementation. Other reasons to consider for the additional lead time would be to get the devices ordered, budget approvals, installation of the devices, and to make sure the device meets the elusive CIP requirements.</p>
<p>Response: Thank you for your comments. The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
Rick Keetch	NRG Energy Power Marketing, Inc.	3	Negative	<p>1. Do you agree that there is a reliability-related need to modify CIP-005-3 – Cyber Security – Electronic Security Perimeters, to provide additional requirements for Cyber Assets used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter) from outside their Electronic Security Perimeter? Yes Comments: None</p> <p>2. Do you agree with the proposed revisions to CIP-005-3? No Comments:</p> <ul style="list-style-type: none"> • R6 – clarify “remote access for operation of unit is not allowed” to be aligned with NERC’s CAN definition “laptop designed with intent or purpose of doing control”. Also suggest an exception for disaster situations. • R6.3.3 – Remove 6.3.3 and add the associated requirements into the existing CIP-005 vulnerability assessment requirement. <p>R6.5.4 – Use of signed and dated acknowledgement of a remote user agreement does not guarantee this practice but rather use of policy and training as a pre-requisite for access would satisfy this concern.</p> <p>3. Do you agree with the proposed implementation language (six months</p>

Voter	Entity	Segment	Vote	Comment
				to comply with the new Requirement R6 after the standard becomes effective)? No Comments: The proposed implementation plan is an aggressive timeline and difficult to achieve. Suggest staged implementation with high risk assets followed by lower risk and implemented over a 2 to 3 year period.
<p>Response: Thank you for your comments.</p> <p>The definition of “support or maintenance” has been created to define the uses of remote access for this requirement. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
Patricia A. Lynch	NRG Energy, Inc.	5	Negative	<ul style="list-style-type: none"> • R6 – clarify “remote access for operation of unit is not allowed” to be aligned with NERC’s CAN definition “laptop designed with intent or purpose of doing control”. Also suggest an exception for disaster situations. • R6.3.3 – Remove 6.3.3 and add the associated requirements into the existing CIP-005 vulnerability assessment requirement. • R6.5,4 – Use of signed and dated acknowledgement of a remote user agreement does not guarantee this practice but rather use of policy and training as a pre-requisite for access would satisfy this concern.
Alan R. Johnson	NRG Energy, Inc.	6		
<p>Response: Thank you for your comments.</p> <p>The definition of “support or maintenance” has been created to define the uses of remote access for this requirement. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement</p>				

Voter	Entity	Segment	Vote	Comment
<p>language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
James R. Keller	Wisconsin Electric Power Marketing	3	Affirmative	<p>While the current standard requirement to allow only ports and services required for operations and monitoring, we agree that there is a lack of clarity on how access for technology support should be managed. This update provides specific guidance in this area.</p> <p>The implementation timeline for CIP-005-4 should be coordinated with the implementation timeline for CIP-002-4, CIP-003-4, CIP-004-4, CIP-006-4, CIP-007-4, CIP-008-4 and CIP-009-4. This will allow registered entities to manage to one consistent version of the standards and related requirements at any given time. This will also provide clarity in which requirements are subject to any given audit.</p>
Linda Horn	Wisconsin Electric Power Co.	5		
<p>Response: Thank you for your comments.</p> <p>The intent of the Drafting Team is to submit the changes to CIP-005-4 such that they can be acted upon by FERC in the same time and by the same final decision as the changes submitted for CIP-002-4.</p>				
Anthony Jankowski	Wisconsin Energy Corp.	4	Affirmative	<p>1. Do you agree that there is a reliability-related need to modify CIP-005-3 – Cyber Security – Electronic Security Perimeters, to provide additional requirements for Cyber Assets used to access Critical Cyber Assets (and other non-critical Cyber Assets within a defined Electronic Security Perimeter) from outside their Electronic Security Perimeter? 1 Yes 0 No Comments:</p> <p>While the current standard requirement to allow only ports and services required for operations and monitoring, we agree that there is a lack of clarity on how access for technology support should be managed. This update provides specific guidance in this area.</p> <p>2. Do you agree with the proposed revisions to CIP-005-3? 1 Yes 0 No Comments:</p>

Voter	Entity	Segment	Vote	Comment
				<p>3. Do you agree with the proposed implementation language (six months to comply with the new Requirement R6 after the standard becomes effective)? 0 Yes 1 No Comments:</p> <p>The implementation timeline for CIP-005-4 should be coordinated with the implementation timeline for CIP-002-4, CIP-003-4, CIP-004-4, CIP-006-4, CIP-007-4, CIP-008-4 and CIP-009-4. This will allow registered entities to manage to one consistent version of the standards and related requirements at any given time. This will also provide clarity in which requirements are subject to any given audit.</p>
<p>Response: Thank you for your comments.</p> <p>The intent of the Drafting Team is to submit the changes to CIP-005-4 such that they can be acted upon by FERC in the same time and by the same final decision as the changes submitted for CIP-002-4.</p>				
Richard Comeaux	LaGen	4	Negative	<p>Do you agree with the proposed revisions to CIP-005-3? No Comments:</p> <ul style="list-style-type: none"> • R6 – clarify “remote access for operation of unit is not allowed” to be aligned with NERC’s CAN definition “laptop designed with intent or purpose of doing control”. <p>Also suggest an exception for disaster situations.</p> <ul style="list-style-type: none"> • R6.3.3 – Remove 6.3.3 and add the associated requirements into the existing CIP-005 vulnerability assessment requirement. <p>R6.5,4 – Use of signed and dated acknowledgement of a remote user agreement does not guarantee this practice but rather use of policy and training as a pre-requisite for access would satisfy this concern</p> <p>Do you agree with the proposed implementation language (six months to comply with the new Requirement R6 after the standard becomes effective)? No Comments:</p> <p>The proposed implementation plan is an aggressive timeline and difficult to achieve. Suggest staged implementation with high risk assets followed by lower risk and implemented over a 2 to 3 year period.</p>

Voter	Entity	Segment	Vote	Comment
<p>Response: Thank you for your comments.</p> <p>The definition of “support or maintenance” has been created to define the uses of remote access for this requirement. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN.</p> <p>The Drafting Team does not believe that an “exception for disaster situations” is necessary in this requirement, since that situation is already covered in the existing “emergency situation” language in CIP-003-4 Requirement R1.1. Including such language here may introduce double jeopardy issues, which the Drafting Team consciously avoided.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>				
Amir Y Hammad	Constellation Power Source Generation, Inc.	5	Negative	<p>Constellation Power Generation is voting negative for the following reasons:</p> <ul style="list-style-type: none"> • Routine changes, such as patch and antimalware deployments, are generally a direct connection to a particular device from the DMZ. Requirement 6.1 should acknowledge “interactive” access explicitly. As written, this requirement could prevent entities from properly maintaining CCAs, lending to a potential threat to the BES. • The changes to CIP-005 are partially covered in other reliability standards and requirements. Requirement 6.3 concentrates on user management and is properly addressed in CIP-004 Requirement 4. Requirement 6.3 appears to overlap and perhaps undermine CIP-004 Requirement 4. Compliance with Requirement 4 of CIP-004 should, by design, demonstrate compliance with the proposed CIP-005 R6.3. Demonstrating compliance twice presents an opportunity for double jeopardy, is redundant, and burdensome. • There are considerable challenges to overcome in order to monitor, record, and maintain the duration of access of each user for every device captured in this requirement, which does not mitigate the risks to or

Voter	Entity	Segment	Vote	Comment
				<p>strengthen the reliability of the BES. Capturing this evidence is labor intensive, cumbersome, and simply not practical and in most cases not technically feasible. The value-add of this requirement is null and it should be omitted.</p> <ul style="list-style-type: none"> • Requirement 6.5 should be omitted in its entirety. As it is currently constructed, the requirement is too prescriptive and is not technically feasible for devices that are not owned by the entity, are outside of the network, and can't be controlled or accessed by the entity. • Finally, encryption should be defined, as it relates to the standard. As written, the standard still reads as a "How-To" to protect devices in and associated with the ESP versus a "What-To" protect in and associated with the ESP. There are several alternatives to protecting devices; therefore entities should be allowed to choose the option(s) which seamlessly coincide with their unique environments.
<p>Response: Thank you for your comments.</p> <p>The definition of "remote access" has been renamed "interactive remote access", and all references updated accordingly.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>A section on encryption has been added to the associated guidance document.</p>				
Brenda Powell	Constellation Energy Commodities Group	6	Negative	<p>The exemption that was "4.2.1 Facilities regulated by the U.S. Nuclear Regulatory Commission or the Canadian Nuclear Safety Commission" should not have been removed.</p> <p>CCG recommends removing R6.3.1 and R6.3.2 because of the double jeopardy with CIP-004 R4 which could result in non-compliance with two standards for a single infraction of the same access control issue. There are considerable challenges to overcome in order to monitor, record, and maintain the duration of access of each user for every device captured in</p>

Voter	Entity	Segment	Vote	Comment
				<p>this requirement, which does not mitigate the risks to or strengthen the reliability of the BES. Capturing this evidence is cumbersome and simply not practical and in most cases not technically feasible. An alternative approach is to log user duration at the access point only. The requirement should be written in a manner that a Technical Feasibility Exception (TFE) is not needed . The value-add of this sub-requirement is null and it should be omitted if it cannot be constructed to exclude TFEs and cumbersome logging.</p> <p>CCG recommends changing R6.4 from “technical controls” to “controls” to allow procedural controls</p>
<p>Response: Thank you for your comments. The Drafting Team agrees with the issue concerning nuclear facilities, and has inserted the language developed for project 2008-06 concerning the nuclear exemption.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p>				
Mike Laney	Luminant Generation Company LLC	5	Negative	Luminant does not believe there is a need for an urgent revision to CIP-005-3. The current standard has requirements in place that adequately address controls and security for remote access to Critical Cyber Assets. Any revisions to CIP-005-3 should be accomplished through the normal Standard Drafting Team activities.
<p>Response: Thank you for your comments. Information provided by the US Government and included in the the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)”, published in March 2010, lead to concerns expressed over insecure remote access configurations; therefore, requirements concerning remote access are necessary. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p>				
David Gordon	Massachusetts Municipal Wholesale Electric Company	5	Negative	Requirement 6.5 and related sub-requirements should be deleted from the proposed revision. Requirement 6.5 adds little to the protection afforded by the proposed requirements 6.1 through 6.4. A remote access user agreement that specifies how the remote user's computer is to be configured and managed would be unenforceable and ineffective at protecting critical cyber assets. Entities should focus their efforts on managing and protecting the assets that they control.
<p>Response: Thank you for your comments. Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added</p>				

Voter	Entity	Segment	Vote	Comment
to the associated guidance document which addresses how the connection requirements can be met.				
Don Schmit	Nebraska Public Power District	5	Affirmative	Note incorrect reference to CIP 004-4 in 6.3.2. Suggest striking 6.5.4 (user agreement) from the Standard.
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Melissa Kurtz	U.S. Army Corps of Engineers	5	Negative	<p>Section 6.1 - We are interpreting this to mean a proxy server is required, however we are not sure of the interpretation. Would a VPN be allowed instead? Proxy servers are not always compatible with non-Windows operating systems. Therefore it may not be feasible for some assets like PLC's and RTU's. This requirement is very burdensome for small sites with 1 or 2 critical assets.</p> <p>Section 6.4.1 - Unclear if multifactor authentication is to VPN or end device. May not be possible if end device as it would require key infrastructure, again PLC's and RTU's may not work with these systems. Very burdensome for small/remote sites.</p>
<p>Response: Thank you for your comments. The SDT believes that an intermediate device (sometimes called a proxy server) is necessary when performing interactive remote access. The proposed Requirement R6 plays no role when non-interactive remote access (e.g., telemetry) is used. Proxy servers are widely available for various operating platforms, including for windows and variants of unix.</p> <p>Requirement R6.3 has been modified to clearly specify that multi-factor authentication is only required to the intermediate device.</p> <p>The technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p>				

Voter	Entity	Segment	Vote	Comment
Leonard Rentmeester	Wisconsin Public Service Corp.	5	Negative	<p>1) 6.5.1 still needs further clarification around whether the intermediate device is to be considered a CCA or treated as a CCA.</p> <p>2) There should be a distinction made between the requirement around remote access outside the PSP vs inside the PSP. When in the office (inside the PSP) internal controls manage the access for tech support by going thru the firewall and citrix then IPS whereas external remote access goes thru a VPN device then firewall then citrix then thru IPS device."</p>
<p>Response: Thank you for your comments. Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p> <p>The current language of the CIP standards only distinguishes between access from within an ESP and access from outside an ESP. There is no distinction given to access which originates from outside an ESP but within a PSP. Requirement R6 does not alter this, and places controls on those Cyber Assets outside the ESP which are used to perform support or maintenance access to Cyber Assets within the ESP.</p>				
Silvia P Mitchell	Florida Power & Light Co.	6	Affirmative	<p>NextEra Energy, Inc "NextEra Energy" believes that in order to help avoid misinterpretation of remote access, a better definition of "remote access" should be defined in the NERC Glossary; as well as a relevant example. The lack of a definition causes ambiguity. As the standard is currently written, Responsible Entities could consider the following questions in order to comply with the standard. It is unclear whether the term "remote access" covers the situation where a person located in one Electronic Security Perimeter (ESP) is accessing cyber assets logically located in another ESP. It is unclear whether the term "remote access" covers the situation where access to a Cyber Asset from another Cyber Asset within the ESP considered remote access? What is the difference between remote access and direct access?</p> <p>Requirement CIP-005 R6.1 specifically states that an intermediate device or proxy system shall be located inside a protected ESP or shall be protected as defined by CIP-005 R1.5. As written, the device can be installed such that the device: 1) Is not a CCA as defined by CIP-002 R3, 2) Is not required to be within an ESP, or 3) Is not covered by R1.5. The device has no protective requirements. NextEra Energy interprets this as different from the intent of the requirement. A better definition of</p>

Voter	Entity	Segment	Vote	Comment
				<p>intermediate device is requested.</p> <p>Regarding Requirement R6.2, a definition of encrypted communications is requested to be included in the NERC Glossary as well.</p> <p>Requirement R6.2.3 does not specify the frequency of the task; therefore, it introduces ambiguity into the requirement which will be interpreted differently by different auditors. An acceptable and reasonable timeframe should be included into the requirement. Requirement R6.2.3 should be reworded to embed the frequency, as such:</p> <p style="padding-left: 40px;">“Annually assess that the technical controls for Remote Access are implemented as authorized and remediate any findings.”</p> <p>For Requirement R6.3, NextEra Energy recommends defining Multifactor Control in the NERC Glossary.</p> <p style="padding-left: 40px;">A reasonable definition to include in the requirement is, “Multi-factor access requires, in addition to the user identification, the use of two or more types of factors. A factor is defined as: 1) what the requestor individually knows as a secret, such as a password, 2) what the requestor uniquely has, such as a physical or software token, an ID-card, or a device that receives via an independent communications channel an authentication token, 3) what the requestor individually is, such as biometric data, like a fingerprint or the face geometry or 4) where the person is located</p> <p>A definition of multi-factor access is requested as well.</p> <p>Requirement R6.3.2 should be included in sub requirement CIP-005 R3.3. since R3 includes "Monitoring Electronic Access" requirements.</p> <p>NextEra Energy recommends re-writing such that logging on individual connection to a cyber asset is not required. This is difficult, almost impossible to achieve technically. The initial access may be to an individual device within the ESP. After the initial access to the remote cyber asset is granted, it is not known where the individual may go from there.</p>

Voter	Entity	Segment	Vote	Comment
				<p>NextEra Energy proposes the rewording of requirement R6.4.3 to read, “Implement, and document the processes for producing and monitoring electronic access logs which contain user identification, login time, and logout or disconnect time of access to the intermediate device or proxy system.</p> <p>NextEra Energy would like clarification concerning requirement R6.5 on whether the cyber assets used to access cyber assets that logically reside within an ESP must adhere to the same levels of protection as those cyber assets within the ESP. Is this the case with portable devices such as laptops? Does implement mean technically implement and enforce? If it is a requirement to separately protect these devices as well, it needs to be determined if the word implement also means enforce. Furthermore, the ability to enforce this is only available from a very limited set of vendors and is beyond the capability of small responsible entities. There are known issues regarding the technical enforcement of this requirement. For example, the remote computers accessing the ESP may not be owned by the entity and therefore is not fully enforceable with technical controls.</p> <p>NextEra Energy would like to propose that for requirement R6.5, the language be modified to “Establish and document an acceptable use policy regarding cyber assets used for remote access that requires....”</p> <p>For R6.5.4, NextEra Energy suggests the following, “The owner of the cyber asset used for remote access is responsible for enforcing the responsible entity's policy.”</p> <p>The implementation period of the new requirement should follow the widely accepted implementation timeframe of two calendar years after the standard becomes effective.</p>
<p>Response: Thank you for your comments. The proposed definition clearly states that “remote access” must be initiated from a Cyber Asset not within an entity’s ESP. If the initiating Cyber Asset is within any of the Responsible Entity’s ESPs, it is not “remote access”.</p> <p>The definition of “interactive remote access” has been modified to specify that communications from the intermediate device to devices within the ESP is not considered interactive remote access. The SDT has attempted to balance the “what” issues with the “how” issues, and feels that the proposed standards (as modified in response to comments) provides a set of requirements, with sufficient flexibility in</p>				

Voter	Entity	Segment	Vote	Comment
<p>implementation.</p> <p>The Drafting Team does not believe a NERC-specific definition for encryption is necessary. A section on encryption has been added to the associated guidance document.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>The companion reference document “Secure Remote Access – Draft” provides an overview of multi-factor authentication. In addition, a footnote reference has been added to the standard.</p> <p>The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment, and to indicate where multi-factor authentication is required. As indicated by the definition of “intermediate device”, if the intermediate device is located outside the Electronic Security Perimeter, there are no requirements placed on the device.</p> <p>For 6.2, there are many accepted methods for encrypted communications; one of the goals of the SDT was to NOT be prescriptive. This issue may be raised again during the future development of the Project 2008-06 SDT.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Nicholas Lauriat	Network & Security Technologies	8	Negative	<p>N&ST suggests revising R6.1 to allow certain remote systems to access Cyber Assets within an ESP directly when all of the following conditions are true:</p> <ul style="list-style-type: none"> (a) The remote system is controlled by the same Responsible Entity as the Cyber Assets within the ESP. (b) There is an operational requirement for direct access. Some activities, such as patching and vulnerability assessments, may be difficult or impossible via an intermediate system. The Responsible Entity should be required to document the operational requirement that makes direct connection necessary. (c) The remote system meets the requirements of R6.5.1, R6.5.2, and R6.5.3. <p>N&ST considers account management Requirements 6.3.1 and 6.3.2 to be redundant and already addressed by existing CIP-005-3 requirement R2.5 (renumbered to R2.4 in proposed CIP-005-4), as well as by CIP-004 Requirement R4. They should be eliminated.</p>

Voter	Entity	Segment	Vote	Comment
				<p>N&ST also considers Requirement R6.3.3 largely addressed by the existing CIP-005 requirement for Cyber Vulnerability Assessment (R4). It should either be eliminated entirely, or any of its provisions that are unique to remote access (such as encryption or 2-factor authentication) should be appended to existing CIP-005 Requirement R4.</p> <p>N&ST does believe requirements R6.5.1, R6.5.2, and R6.5.3 can and should be applied to remote systems with direct access to systems within the ESP. However, we believe they should not be applied to indirectly connected systems that are under the Responsible Entity's control.</p> <p>We also believe that NONE of requirements R6.5.1 through R6.5.4 should apply to remote systems that are NOT under the Responsible Entity's control or are not used to connect to the ESP. This recommendation is based on our belief that as written the requirements are unenforceable and cannot be audited. A signed and dated acknowledgement form would, in our opinion, prove nothing.</p>
<p>Response: Thank you for your comments.</p> <p>The current language of the CIP standards only distinguishes between access from within an ESP and access from outside an ESP. Requirement R6 does not alter this, and places controls on those Cyber Assets outside the ESP which are used to perform support or maintenance access to Cyber Assets within the ESP.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the "CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)" released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Larry D. Grimm	Texas Reliability Entity	10	Negative	<p>Requirement R6.4.2 is considered to be a key control and is properly included in this standard, but it does not go far enough. The standard should require access logs to be periodically reviewed on a frequent basis, not merely accumulated.</p> <p>(1) In Requirement 6.3, the "procedural controls" (R6.3) and "technical controls" (R6.4) should be "approved" controls. These controls should be approved by an appropriate level of entity management, and not merely</p>

Voter	Entity	Segment	Vote	Comment
				<p>“established, implemented and documented” by IT or security staff.</p> <p>(2) R6.4.2 should require a process for “periodically monitoring” the electronic access logs of remote access. These logs should be reviewed on a regular basis, preferably daily or weekly. It is unacceptable to allow suspicious or unacceptable access to continue for days or longer due to failure to review the access logs.</p> <p>(3) R6.5.4 should require an “annual acknowledgement of the remote access user agreement by all remote access users.” This acknowledgement should be signed at least annually in order to remind all remote access users of their obligations and to provide a periodic review of compliance with the requirements of the agreement.</p>
<p>Response: Thank you for your comments.</p> <p>Requirements R6.3 and 6.4 have been modified to remove double-jeopardy (i.e., potential non compliance with multiple requirements for the same issue) issues, and in response to this and other comments.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Louise McCarren	Western Electricity Coordinating Council	10	Affirmative	<p>WECC thanks the drafting team for the way in which they addressed comments from the last posting. Many of our concerns have been addressed in a satisfactory way. WECC is voting to approve this version of the standard, but still has concerns as noted below.</p> <p>We recommend that from an auditing perspective, and for clarification, the language of R2.4 would be improved by modifying it to read “The required CIP-005 R2 COMPLIANCE DOCUMENTATION shall, at least, identify and describe:”</p> <p>We believe that the intent of R6.2 is to PROTECT communications between the Cyber Asset performing remote access and the intermediate device. However, as worded the requirement only requires encryption. From an auditor’s perspective a responsible entity could be utilizing an encryption method that had been proven to be broken, thus</p>

Voter	Entity	Segment	Vote	Comment
				<p>offering no protection, and yet the responsible entity would be able to argue that they met the requirement.</p> <p>We suggest changing the language of R6.2 to “Implement the remote access system such that communications between the Cyber Asset performing remote access and the intermediate device are PROTECTED BY ENCRYPTION while the communications traverse ...”</p> <p>This would require the desired protection by encryption.</p> <p>We also recommend that R6.5 should include a reference that the remote access user policy shall be represented in the responsible entity’s overall Cyber Security Policy developed pursuant to CIP-003 R1.</p>
<p>Response: Thank you for your comments.</p> <p>The scope of this Drafting Team’s responsibility is the new Requirement R6 (and the associated removal of the former Requirement R2.4).</p> <p>The Drafting Team does not believe the phrase “protected by encryption” adds clarity to the requirement. A section on encryption has been added to the associated guidance document.</p> <p>Regarding R6.5, the requirement has been rewritten in response to this and other comments, in particular to remove the end-user agreement language, insert a requirement for contractual language for vendors, contractors, and consultants which addresses the technical controls to be applied. Based on issues raised in the “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010, the SDT believes that the prohibition on split tunneling and dual homing is still required even when an intermediate device is used. A section has been added to the associated guidance document which addresses how the connection requirements can be met.</p>				
Joseph O'Brien	Northern Indiana Public Service Co.	6	Negative	See comment form under "Posted for Comment"
Richard Burt	Minnkota Power Coop. Inc.	1	Negative	See comments submitted by MRO NSRS.
R Scott S. Barfield-McGinnis	Georgia System Operations Corporation	3	Negative	See GSOC & GTC formal comment document.
Guy Andrews	Georgia System Operations Corporation	4	Negative	See GSOC & GTC Formal Comment Document

Voter	Entity	Segment	Vote	Comment
Gregory S Miller	Baltimore Gas & Electric Company	1	Negative	Please refer to BGE's comments submitted in conjunction with this ballot.
Harold Taylor, II	Georgia Transmission Corporation	1	Negative	Please refer to our comment response filed via the formal comment form.
Chuck B Manning	Electric Reliability Council of Texas, Inc.	2	Negative	ERCOT ISO has filed comments through the online form. Please reference filed comments for details.
Michael Mertz	PNM Resources	3	Negative	See comment form submitted on behalf of PNM Resources
Brenda L Truhe	PPL Electric Utilities Corp.	1	Affirmative	PPL Electric Utilities submitted comments on Project 2010-15 via the comment form on 12/10/2010.
Horace Stephen Williamson	Southern Company Services, Inc.	1	Negative	See comments filed for CIP-005-3 (Project 2010-15) for Southern Company.
Richard J. Mandes	Alabama Power Company	3		
Don Horsley	Mississippi Power	3		
Anthony L Wilson	Georgia Power Company	3		
Gregory L Pieper	Xcel Energy, Inc.	1	Negative	Xcel Energy will submit detail comments separate from the ballot.
Michael Ibold	Xcel Energy, Inc.	3	Negative	Please see our detail comments.
Liam Noailles	Xcel Energy, Inc.	5	Negative	please see our detail comments (We will submit detail comments separate from the ballot)
David F. Lemmons	Xcel Energy, Inc.	6	Negative	Please refer to our detailed comments submitted through the comment process.

Response: Thank you for your comments. Please refer to our responses in the comment document.

