

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

**Summary Consideration:**

Most commenters noted that the VSLs needed to be modified based on changes to the requirements. The VSLs were updated to reflect the changed requirements language.

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](mailto:herb.schrayshuen@nerc.net). In addition, there is a NERC Reliability Standards Appeals Process.<sup>1</sup>

Kirit S. Shah	Ameren Services	1	Negative	We believe that the language of several requirements would change. This may then require VRF and VSL changes.
<b>Response:</b> Thank you for your comments. The language of the VSLs has been updated to reflect changes in the requirements.				
Paul B. Johnson	American Electric Power	1	Negative	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.  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.  AEP contends that R6.5 and applicable sub-requirements are paperwork related
Edward P. Cox	AEP Marketing	6	Negative	

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

				<p>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>
<p><b>Response:</b> Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report.</p>				
<p>The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.</p>				
Douglas E. Hils	Duke Energy Carolina	1	Negative	<p>Below are our comments related to the draft document. 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:</p> <ul style="list-style-type: none"> <li>• Second paragraph of R6 -- Strike the word "monitoring" in order to avoid ambiguity with monitoring of equipment other than Cyber Assets.</li> <li>• 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".</li> <li>• Requirement 6.3.3 -- This section addresses assessment of technical controls, and should be moved to R6.4 and renumbered R6.4.3.</li> <li>• 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.</li> </ul>
<p><b>Response:</b> Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.</p>				
David Batz	Edison Electric Institute	1	Abstain	EEI supports efforts to add additional controls for remote access to Electronic Security.
<p><b>Response:</b> Thank you for your supportive comments.</p>				

Robert Martinko	FirstEnergy Energy Delivery	1	Negative	FE approves the Medium VRF level and the VSLs are largely acceptable as written. We are voting against due to the reference and inclusion of sub-requirement R6.5.4 within the VSL assignments. Please refer to our ballot comments on the CIP-005-4 regarding our concerns with R6.5.4.
Kevin Query	FirstEnergy Solutions	3	Negative	
Douglas Hohlbaugh	Ohio Edison Company	4	Negative	
Kenneth Dresner	FirstEnergy Solutions	5	Negative	
Mark S Travaglianti	FirstEnergy Solutions	6	Negative	
<b>Response:</b> Thank you for your comments. Please refer to our responses in the comment document. The language of the VSLs has been updated to reflect changes in the requirements.				
Joe D Petaski	Manitoba Hydro	1	Negative	NERC should make available the previous BOT approved version of the CIP-005-3 VSLs and VRFs for industry to assist in preparing voting responses on the proposed version. The VSLs for the proposed CIP-005-4 were not updated to match the language in the most recent version (December 1 2010) of the standard posted on for ballot. The standard refers to a "remote access user policy", not an "acceptable use policy" as indicated in the VSLs. "responsible entity" should be capitalized.
Greg C. Parent	Manitoba Hydro	3	Negative	
S N Fernando	Manitoba Hydro	5	Negative	
Daniel Prowse	Manitoba Hydro	6	Negative	
<b>Response:</b> Thank you for your comments. Since Requirement R6 is new, there are no prior VRF or VSLs for that requirement. Please refer to our responses in the comment document. The language of the VSLs has been updated to reflect changes in the requirements.				
Randy MacDonald	New Brunswick Power Transmission Corporation	1	Negative	The draft standard shows the removal of the Canadian nuclear exclusion
<b>Response:</b> Thank you for your comments. This comment was also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.				
Michael T. Quinn	Oncor Electric Delivery	1	Negative	Regarding the Severe VSL: 1) Revise the wording to match the language of the requirement, "failed to implement an intermediate device or proxy system such that the Cyber

				<p>Asset performing remote access does not have direct network access to Cyber Asset(s) within an the Electronic Security Perimeter.”</p> <p>2) Revise the wording to match the language of the requirement, “failed to 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, as defined in Requirement 6 Part 6.2.”</p>
<p><b>Response:</b> Thank you for your comments. The VSLs need to be written in the past tense, while the requirement is written in the active voice. Thus, in this instance, the differences in wording between the requirements and the VSLs are appropriate.</p>				
John C. Collins	Platte River Power Authority	1	Negative	<p>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:</p> <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:</p> <p style="padding-left: 40px;">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</p>
Terry L Baker	Platte River Power Authority	3	Negative	
Pete Ungerman	Platte River Power Authority	5	Negative	
Carol Ballantine	Platte River Power Authority	6	Negative	

			<p>Cyber Asset(s) within the Electronic Security Perimeter.  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.  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:  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.  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:  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</p>
--	--	--	--

			<p>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 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>
--	--	--	--

**Response:** Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.

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. 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? It is recommended that it is to the jump server located within the ESP.</p>
Marjorie S. Parsons	Tennessee Valley Authority	6	Negative	

				<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><b>Response:</b> Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.</p>				
John Tolo	Tucson Electric Power Co.	1	Negative	The current VRFs and VSLs are adequate.
<p><b>Response:</b> Thank you for your positive comments.</p>				
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.
<p><b>Response:</b> Thank you for your comments. Please see our response to your concerns in the comment report for the ballot of the proposed standard.</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 comment form for this posting.
<p><b>Response:</b> Thank you for your comments. This comment was also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.</p>				
Jason L Marshall	Midwest ISO, Inc.	2	Negative	We believe additional changes are necessary to the standards before the VSLs can be finalized. Furthermore, we think the importance of the requirement is factoring into the VSLs. It should not. For instance, any failure with establishing procedural controls appears to move to a Severe VSL. However, even without procedural controls, a responsible entity could meet the intent of the requirement. It certainly would be more challenging but still possible. Thus, failure to establish procedural controls does not cause a responsible entity to automatically miss the majority of the requirement. Failure to miss two sub-requirements should not be a High VSL but rather a Moderate VSL. Missing three sub-requirements might be a High VSL. Failure to miss one sub-requirement should not be Moderate VSL. It should be a Lower VSL. We can support a Medium VRF.

<b>Response:</b> Thank you for your comments. Noncompliant performance that meets the threshold for a “Severe” VSL is performance that mostly or completely misses the reliability intent of the associated requirement – an entity does not need to be 100% noncompliant for that noncompliance to be assigned a Severe VSL.				
Russell A Noble	Cowlitz County PUD	3	Affirmative	Should not the VSL parallel the wording of the requirement? Suggest the following: "failed to include one of the elements in Requirement 6 Part 6.4.1 through 6.4.2 in its technical controls to prevent unauthorized individuals from establishing remote access"
<b>Response:</b> Thank you for your comments. Please refer to our responses in the comment document. The language of the VSLs has been updated to reflect changes in the requirements.				
Michael Mertz	PNM Resources	3	Negative	See comment form submitted on behalf of PNM Resources for Expedited Revisions to CIP-005-3
<b>Response:</b> Thank you for your comments. Please refer to our responses in the comment document.				
Rick Syring	Cowlitz County PUD	4	Affirmative	VSL for 6.4 uses the word "ensure" rather than "prevent"
<b>Response:</b> Thank you for your comments. The language of the VSLs has been updated to reflect changes in the requirements.				
Bob Essex	Cowlitz County PUD	5	Affirmative	VSLs for subrequirement 6.4 does not use similar wording the requirement uses. Suggest "...protect against unauthorized access..." rather than "ensure."
<b>Response:</b> Thank you for your comments. The language of the VSLs has been updated to reflect changes in the requirements.				
Patricia A. Lynch	NRG Energy, Inc.	5	Negative	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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. 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.</li> </ul>

<b>Response:</b> Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.				
Joseph O'Brien	Northern Indiana Public Service Co.	6	Negative	See comment form under "Posted for Comment"
<b>Response:</b> Thank you for your comments. Please refer to our responses in the comment document.				
Donald E. Nelson	Commonwealth of Massachusetts Department of Public Utilities	9	Negative	<p>The Canadian nuclear exclusion must be included. The associated guidance document Secure Remote Access--Draft should have an explicit disclaimer that it will not be used for audit purposes.</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> <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>
<b>Response:</b> Thank you for your comments. These comments were also submitted with the ballot for the proposed standard. Please see the response to those comments in the standard ballot report. The purpose of this non-binding poll was to collect feedback on the VRFs and VSLs that were proposed.				
Guy V. Zito	Northeast Power Coordinating Council, Inc.	10	Negative	Due to the NPCC suggestions made to revise the standard's requirements, NPCC can not support the VSLs as written.
<b>Response:</b> Thank you for your comments. Please refer to our responses in the comment document. The language of the VSLs has been updated to reflect changes in the requirements.				
Anthony E Jablonski	ReliabilityFirst Corporation	10	Negative	<p>ReliabilityFirst agrees with the Violation Risk Factor but disagrees with the Violation Severity Levels for R6 based on the following reasons:</p> <p>1. The end of R6 states "in the following sub requirements" while the associated VSLs refers to "parts." The requirements or VSLs need to be modified for</p>

				<p>consistency.</p> <p>2. The first VSL under the "Severe" category should reference Part 6.1</p> <p>3. The third VSL under the "Severe" category should reference Part 6.3</p> <p>4. The fourth VSL under the "Severe" category should reference Part 6.4</p> <p>5. The fifth VSL under the "Severe" category should reference Part 6.5</p> <p>6. The last VSL under the all four VSL categories uses the term "acceptable use policy." Requirement 6 (or related sub requirements) does not have any language stating "acceptable use policy." This is a violation of the FERC Guideline 3: "Violation Severity Level Assignment Should Be Consistent with the Corresponding Requirement"</p>
<p><b>Response:</b> Thank you for your comments. The standard was updated following a Quality Review on December 1, 2010, and some, but not all of the elements of the VSLs were updated with conforming changes. The language of the VSLs has been updated to reflect changes in the requirements.</p>				

END OF REPORT