

Consideration of Comments on Urgent Action Revisions to CIP-005-3 – Project 2010-15

The Urgent Action Revisions to CIP-005-3 – CIP-005 Drafting Team thanks all commenters who submitted comments on the proposed revisions (clean and redline) to the CIP-005-3 Cyber Security --- Electronic Security Perimeters. These standards were posted for a 30-day public comment period from November 12, 2010 through December 11, 2010. The stakeholders were asked to provide feedback on the standards through a special Electronic Comment Form. There were 14 sets of comments, including comments from more than 75 different people from approximately 45 companies representing 8 of the 10 Industry Segments as shown in the table on the following pages.

http://www.nerc.com/filez/standards/SAR-Urgent_Action_Revisions%20to%20CIP-005-3.html

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 your comment has been overlooked, 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

¹ The appeals process is in the Reliability Standards Development Procedures:
<http://www.nerc.com/standards/newstandardsprocess.html>.

Index to Questions, Comments, and Responses

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?.....	10
2. Do you agree with the proposed revisions to CIP-005-3?	19
3. Do you agree with the proposed implementation language (six months to comply with the new Requirement R6 after the standard becomes effective)? ⁶²	
END OF REPORT	68

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

The Industry Segments are:

- 1 — Transmission Owners
- 2 — RTOs, ISOs
- 3 — Load-serving Entities
- 4 — Transmission-dependent Utilities
- 5 — Electric Generators
- 6 — Electricity Brokers, Aggregators, and Marketers
- 7 — Large Electricity End Users
- 8 — Small Electricity End Users
- 9 — Federal, State, Provincial Regulatory or other Government Entities
- 10 — Regional Reliability Organizations, Regional Entities

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
1.	Group	Guy Zito	Northeast Power Coordinating Council	10									
1.	Al Adamson	New York State Reliability Council, LLC	NPCC	10									
2.	Gregory Campoli	New York Independent System Operator	NPCC	2									
3.	Kurtis Chong	Independent System Operator	NPCC	2									
4.	Sylvain Clermont	Hydro-Quebec TransEnergie	NPCC	1									
5.	Chris de Graffenried	Consolidated Edison Co. of New York, Inc.	NPCC	1									
6.	Gerry Dunbar	Northeast Power Coordinating Council	NPCC	10									
7.	Dean Ellis	Dynegy Generation	NPCC	5									
8.	Brian Evans-Mongeon	Utility Services	NPCC	8									
9.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5									
10.	Kathleen Goodman	ISO - New England	NPCC	2									
11.	Chantel Haswell	FPL Group, Inc.	NPCC	5									
12.	David Kiguel	Hydro One Networks Inc.	NPCC	1									
13.	Michael R. Lombardi	Northeast Utility	NPCC	1									
14.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10									
15.	Robert Pellegrini	The United Illuminating Company	NPCC	1									

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Group/Individual	Commenter	Organization	Registered Ballot Body Segment											
			1	2	3	4	5	6	7	8	9	10		
16. Randy MacDonald	New Brunswick System Operator	NPCC 2												
17. Saurabh Saksena	National Grid	NPCC 1												
18. Michael Schiavone	National Grid	NPCC 1												
19. Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC 3												
20. Si Truc Phan	Hydro-Quebec TransEnergie	NPCC 1												
21. Bruce Metruck	New York Power Authority	NPCC 6												
22. Brian L. Gooder	Ontario Power Generation Incorporated	5												
2.	Group	Denise Koehn	Bonneville Power Administration		1, 3, 5 and 6									
1. Forrest Krigbaum	BPA, Transmission, System Operations	WECC 1												
2. James Phillips	BPA, Transmission, System Operations	WECC 1												
3. Kelly Hazelton	BPA, Transmission, System Operations	WECC 1												
4. Tom Gist	BPA, Transmission, CC HW Dsgn/Std Monr & Admin	WECC 1												
5. John Wylder	BPA, Transmission, CC HW Dsgn/Std Monr & Admin	WECC 1												
6. Kevin Dorning	BPA, Transmission, PSC Technical Svcs	WECC 1												
7. Sharon Brown	BPA, Transmission, Project and Planning Support	WECC 1												
8. Rene Dominguez	Transmission, System Operations	WECC 1												
3.	Group	Mike Garton	Electric Market Policy		1, 3, 5 and 6									
1. Michael Gildea	Dominion Resources Services, Inc.	NPCC 5, 6												
2. Louis Slade	Dominion Resources Services, Inc.	SERC 5, 6												
3. Bruce Bingham	Dominion Resources Services, Inc.	MRO 5												
4. Greg Dodson	Dominion Resources Services, Inc.	RFC 5												
5. John Loftis	Dominion Virginia Power	SERC 1, 3												
4.	Group	Sasa Maljukan	Hydro One Networks		1									
1. David Kiguel	Hydro One Networks Inc.	NPCC 1												
5.	Group	Carol Gerou	MRO's NERC Standards Review		10									

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
			Subcommittee										
1.	Mahmood Safi	Omaha Public Utility District	MRO 1, 3, 5, 6										
2.	Chuck Lawrence	American Transmission Company	MRO 1										
3.	Tom Webb	WPS Corporation	MRO 3, 4, 5, 6										
4.	Jason Marshall	Midwest ISO Inc.	MRO 2										
5.	Jodi Jenson	Western Area Power Administration	MRO 1, 6										
6.	Ken Goldsmith	Alliant Energy	MRO 4										
7.	Alice Ireland	Xcel Energy	MRO 1, 3, 5, 6										
8.	Dave Rudolph	Basin Electric Power Cooperative	MRO 1, 3, 5, 6										
9.	Eric Ruskamp	Lincoln Electric System	MRO 1, 3, 5, 6										
10.	Joseph Knight	Great River Energy	MRO 1, 3, 5, 6										
11.	Joe DePoorter	Madison Gas & Electric	MRO 3, 4, 5, 6										
12.	Scott Nickels	Rochester Public Utilities	MRO 4										
13.	Terry Harbour	MidAmerican Energy Company	MRO 1, 3, 5, 6										
14.	Richard Burt	Minnkota Power Cooperative, Inc.	MRO 1, 3, 5, 6										
6.	Group	Glen Hatstrup	Kansas City Power & Light	1, 3, 5 and 6									
1.	Michael Gammon	KCPL SPP 1, 3, 5, 6											
2.	Scott Harris	KCPL SPP 1, 3, 5, 6											
3.	Karl Bodenheimer	KCPL SPP 1, 3, 5, 6											
7.	Individual	Mike Haynes	Seattle City Light	X		X	X	X	X				
8.	Individual	Paul McClay	Tampa Electric	X		X	X	X					
9.	Individual	Christine Hasha	Electric Reliability Council of Texas, Inc.		X								
10.	Individual	Sandra Shaffer	PacifiCorp	X		X		X	X				

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
11.	Individual	Janet Smith	Arizona Public Service Company	X		X		X					
12.	Individual	Guy Andrews	Georgia System Operations Corp & Georgia Transmission Corp	X		X	X						
13.	Individual	Silvia Parada Mitchell	NextEra Energy	X		X		X	X				
14.	Individual	JT Wood	Southern Company Transmission	X		X							
15.	Individual	Michael Lombardi	Northeast Utilities	X		X		X					
16.	Individual	Joe Petaski	Manitoba Hydro	X		X		X	X				
17.	Individual	Melissa Kurtz	US Army Corps of Engineers - Omaha District					X					
18.	Individual	Marc Child	Great River Energy	X		X		X	X				
19.	Individual	John Kutzer	Consultant								X		
20.	Individual	Michael Mertz	PNM Resources	X		X		X					
21.	Individual	Dan Roethemeyer	Dynegy Inc.					X					
22.	Individual	Joe O'Brien for Tim Conway	NIPSCO	X		X		X	X				
23.	Individual	Glen Hatstrup	Kansas City Power & Light	X		X		X					
24.	Individual	Todd Williams	MidAmerican Energy Company	X		X		X	X				

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
25.	Individual	Greg Rowland	Duke Energy	X		X		X	X				
26.	Individual	Jonathan Appelbaum	United Illuminating	X									
27.	Individual	Ed Davis	Entergy Services	X		X		X	X				
28.	Individual	John Bee	Exelon	X				X					
29.	Individual	Bill Keagle	BGE	X									
30.	Individual	John Brockhan	CenterPoint Energy	X		X							
31.	Individual	Thad Ness	American Electric Power	X		X		X	X				
32.	Individual	Doug Hohlbaugh	FirstEnergy	X		X	X	X	X				
33.	Individual	Candace Morakinyo	Wisconsin Electric Power Company d/b/a We Energies			X	X	X	X				
34.	Individual	Brenda Truhe	PPL Electric Utilities	X									
35.	Individual	Andrew Pusztai	American Transmission Company	X									
36.	Individual	Kirit S. Shah	Ameren	X		X		X	X				
37.	Individual	Saurabh Saksena	National Grid	X		X							
38.	Individual	David S. Revill	Georgia Transmission Corporation	X									
39.	Individual	Kathleen Goodman	ISO New England		X								

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Group/Individual		Commenter	Organization	Registered Ballot Body Segment										
				1	2	3	4	5	6	7	8	9	10	
40.	Individual	Jason Marshall	Midwest ISO		X									
41.	Individual	Darryl Curtis	Oncor Electric Delivery	X										
42.	Individual	Gregory Campoli	New York Independent System Operator		X									
43.	Individual	Louise McCarren	WECC											X
44.	Individual	Dan Rochester	Independent Electricity System Operator		X									
45.	Individual	Adam Menendez	Portland General Electric Company	X		X		X	X					

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?

Summary Consideration:

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, as is noted in the Disclaimer section of the guidance document “[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.”

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 that the proposed requirements was in conflict with or duplicative of CAN-0005. The Drafting Team responded that the new Requirement R6 was complementary to the issue raised in CAN-0005.

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

Organization	Yes or No	Question 1 Comment
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	Yes	
Electric Market Policy	Yes	In general, Dominion supports the following measures when using a routable protocol for remotely accessing cyber assets within an ESP:

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
		<ul style="list-style-type: none"> • Multifactor authentication for interactive access. • A prohibition on dual-homing and split-tunneling. • Introduction of an intermediate device or system so interactive access from an external device does not communicate directly with a cyber asset within an ESP. • Use of encryption from a remote device to an ESP access point. • Requiring that 1) anyone granted remote access to an ESP has access to protected devices inside the ESP, and 2) removal of access to all devices inside an ESP requires removal of remote access to the ESP.
<p>Response: Thank you for your comments.</p>		
Hydro One Networks	Yes	
MRO's NERC Standards Review Subcommittee	Yes	N/A
Kansas City Power & Light	Yes	
Seattle City Light	Yes	
Tampa Electric	No	<p>We believe that the proposed changes to CIP005 go beyond and are possibly in conflict with FERC's direction in order 706, paragraph 511. FERC directed only that NERC provide additional guidance, beyond that provided in the version 1 standard and frequently asked questions, as to what constitutes "strong authentication". This could be accomplished through a guidance document, or the addition of a definition for "strong authentication" to the NERC glossary of terms, rather than a change to the standards. In order 706, FERC also clarified that its intent was not to be prescriptive, but to provide examples, and not limit authentication to specific options, which this SAR and the proposed changes to the standard would effectively do.</p> <p>Furthermore, we believe that the term "external interactive access into the Electronic Security Perimeter" already includes remote access as intended by this SAR. If this term lacks sufficient clarity to be consistently interpreted by the industry, we would recommend the addition of a definition of "external interactive access" to the NERC glossary of terms.</p> <p>From a related administrative perspective, as a general practice NERC should consider the administrative impact to the industry of re-numbering requirements. In this case, requirement 2.4 is being obsoleted and</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
		<p>requirements 2.5 and above are being renumbered. While from an aesthetic point of view this might be preferable, NERC should consider the impact to the industry of this seemingly minor change. Any and all documentation and evidence related to compliance with the old requirement will need to be maintained for audit compliance purposes. Current documentation and evidence related to requirements 2.5 and above will all need to be renumbered. The ongoing tracking and maintenance of this documentation becomes problematic as the historical compliance evidence for a given requirement will not easily align with the current compliance evidence. In some cases this could have even further impacts (TFEs, compliance self certification forms, violations, etc). While this might appear trivial, it creates confusion and unnecessary administrative burden on the part of responsible entities. In cases like this NERC should consider simply obsoleting the old requirement number and not replacing or renumbering other affected requirements.</p>
<p>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.</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 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 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 Electronic Security Perimeter. 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.</p> <p>When a requirement is deleted the numbering of the requirements is automatically adjusted. This is a standard practice for all NERC standards. Your suggestion has been forwarded to NERC’s Director of Standards Process for consideration.</p>		
Electric Reliability Council of Texas, Inc.	No	<p>Through a proper implementation of the controls documented in CIP-005-3, 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</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
		<p>pandemic planning, as well as operations in adverse weather. Request that the drafting team write the requirements or provide an interpretation to CIP-005-3 to address the principles of sound remote access capabilities rather than being prescriptive through the drafting of new requirements.</p>
<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. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p>		
PacifiCorp	No	<p>PacifiCorp does not consider there to be a reliability-related need to supplement CIP-005-3 with additional security requirements on devices used for remote access. Fully patched computers with the most advanced anti-virus software can still be compromised. To that end, PacifiCorp already operates under the assumption that every remote device is potentially hostile and utilizes hardware token-based two factor authentication, no-split-tunneling VPN client configuration, network-based intrusion detection, strict least privilege applied to network ports/protocols, and rigorous logging and monitoring of user access. As such, the existing requirements in CIP-005-3 are sufficient to develop the measures necessary to secure a remote access environment.</p>
<p>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)”. The US Government expressed concern over insecure remote access configurations as expressed in that bulletin; therefore, requirements concerning remote access are necessary.</p>		
Arizona Public Service Company	Yes	
Georgia System Operations Corp & Georgia Transmission Corp	Yes	
NextEra Energy	Yes	
Southern Company Transmission	Yes	<p>Southern is supportive of NERC’s efforts to refine CIP-005-3. However, the existing draft needs additional work to address remote access and to supersede CAN notices regarding this topic. Southern also recommends holding a workshop with the industry to further refine the proposed language, take and respond to questions, and address concerns.</p>
<p>Response: Thank you for your comments. This standards activity is not intended to supersede CAN-0005, but rather to complement it by addressing issues not included within the CAN. Although NERC has not conducted a formal workshop sponsored by this SDT, there have been numerous conference calls via groups</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
like EEI, The Transmission Forum, etc. that have provided valuable informal input during the development of the proposed revisions to CIP-005.		
Northeast Utilities		
Manitoba Hydro	Yes	
US Army Corps of Engineers - Omaha District	Yes	
Great River Energy	No	I believe the existing version 3 offers enough leeway in allowing a responsible entity to manage remote access in a secured manner and customized for their specific environment, to ensure availability and reliability of the critical asset in question.
<p>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)”. The US Government has concerns over insecure remote access configurations as expressed in that bulletin; therefore, requirements concerning remote access are necessary.</p>		
Consultant	Yes	However, the changes indicated are not separate from R2. These changes are a subset of the concepts in R2. A more appropriate title for R2 is "Remote Electronic Access Controls".
<p>Response: Thank you for your comments. Requirement R2 is focused on the requirements of the “electronic access points” (i.e., firewalls) that comprise the Electronic Security Perimeter, and manage all access between Cyber Assets within the Electronic Security Perimeter, and those outside the Electronic Security Perimeter. R2 is outside the scope of work in the approved SAR for this project. The new R6 is focused on requirements placed on the Cyber Assets that initiate and manage interactive remote access.</p>		
PNM Resources	Yes	
Dynergy Inc.	Yes	
NIPSCO	Yes	
Kansas City Power & Light	Yes	Strictly speaking, these changes do not affect reliability. However, the proposed changes are welcomed and provide a more descriptive minimum that must be met by all Responsible Entities.
<p>Response: Thank you for your comments.</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
MidAmerican Energy Company	No	<p>The joint intelligence products from DOD, DOE, Homeland Security and NERC identify opportunities to strengthen cyber access. Additional requirements are not necessary. Modification of existing requirements would meet the need.</p> <p>However, 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 obsolesces technologically faster than the 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.</p> <p>Instead, improvements to CIP standards should be “what” is to be accomplished.</p>
<p>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.</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>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. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p> <p>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 Electronic Security Perimeter. 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.</p> <p>The use of anti-virus with signatures is consistent with the language in CIP-007. Future standards development work by the Project 2008-06 CSO 706 drafting team may change this concept, and if so, will make global changes to consistently address the issue.</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>		
Duke Energy	Yes	
United Illuminating	No	This question highlights a concern UI has regarding the status of the intermediate proxy device being contemplated by R6. The question implies that R6 provides additional requirements for cyber assets used to

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
		<p>access Critical Cyber Assets.</p> <p>If this device contemplated by R6 is considered to be providing access control and monitoring to the ESP then it must be protected per Cip-05 R1.5. UI does not believe that in every implementation of a proxy device that it is controlling access to the ESP. In some implementations a Firewall appliance will provide access control and monitoring to the ESP, and the proxy device s only preventing a direct connection to the ESP.</p>
<p>Response: Thank you for your comments. Former Requirement R2.4 only deals with the requirements placed on access through the Electronic Security Perimeter. 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.</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. 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>		
Energy Services	Yes	
Exelon	Yes	
BGE	Yes	BGE agrees there is a reliability-related need to modify CIP-005-3.
<p>Response: Thank you for your comments.</p>		
CenterPoint Energy	No	<p>CenterPoint Energy does not agree that there is a reliability-related need to modify CIP-005-3. The Company considers the concepts noted in the current draft above and beyond best practice for remote access security. Responsible Entities may choose to enhance remote access controls based on existing and newly discovered vulnerabilities (ex. CIP Awareness Bulletin -- Joint Product -- Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)) with existing and newly available technologies.</p>
<p>Response: Thank you for your comments. The US Government expressed concern over insecure remote access configurations as expressed in the referenced “CIP Awareness Bulletin - Joint Product - Remote Access Attacks: Advanced Attackers Compromise Virtual Private Networks (VPNs)” released in March of 2010 as 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.</p>		
American Electric Power	Yes	<p>Overall, AEP supports the improvements contained in this project, but AEP would like some further refinements as established in our comments below.</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
Response: Thank you for your comments. Please see our responses to your other comments.		
FirstEnergy	Yes	
Wisconsin Electric Power Company d/b/a We Energies	Yes	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.
Response: Thank you for your comments.		
PPL Electric Utilities	Yes	
American Transmission Company	Yes	
Ameren	Yes	
National Grid	Yes	
Georgia Transmission Corporation	Yes	
ISO New England	Yes	
Midwest ISO	Yes	
Oncor Electric Delivery	No	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

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 1 Comment
		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. The goal of the SDT is to provide sufficient clarity in CIP-005-4 to address this problem.</p> <p>Former Requirement R2.4 only deals with the requirements placed on access through the Electronic Security Perimeter. 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.</p>		
New York Independent System Operator	Yes	
WECC	Yes	
Independent Electricity System Operator	Yes	
Portland General Electric Company	Yes	

2. Do you agree with the proposed revisions to CIP-005-3?

Summary Consideration:

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, as stated in the disclaimer section of the guideline: “This 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.”

Many commenters requested the reinstatement of the nuclear exemption language, either for Canadian or US nuclear facilities. These exemptions have been re-inserted.

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 that no technical feasibility language was available in the new Requirement R6. TFE allowance has been provided for dial-up encryption and multi-factor authentication (R6.2).

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

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	<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. 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 deleted 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. The SDT agrees with the issue concerning nuclear facilities, and has inserted the language developed for project</p>		

Organization	Yes or No	Question 2 Comment
		<p>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 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>
Bonneville Power Administration	No	<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> <ol style="list-style-type: none"> 1. Remote Access: Needs simplification - Recommended Change: “Remote access, for the purposes of this requirement and its sub-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).” 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>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>		

Organization	Yes or No	Question 2 Comment
Electric Market Policy	No	<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> <p>Dominion proposes either one of the following language options in order of preference:</p> <p>1) Alter the definition of remote access to specifically exclude dial-up connections:</p> <p style="padding-left: 40px;">Remote access, for the purpose of CIP-005-4 and its subrequirements, is 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) and is exclusive of dial-up access. Remote access can be initiated from: 1) Cyber Assets owned by the Responsible Entity, 2) Cyber Assets owned by employees, contractors, or vendors.</p> <p>2) Alter CIP-005-4-R6 to include “where technically feasible”</p> <p>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 where technically feasible.</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 definition has been updated to reflect this.</p> <p>Requirements R1.1 and R1.2 deal with establishing Electronic Security Perimeters (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>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
Hydro One Networks	No	<p>This draft removes the exclusion of Canadian nuclear facilities. Just to remind you, 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>In addition to this we recommend that requirements 6.3.1 and 6.3.2 be removed. R6.3.1 and R6.3.2 could possibly present a double jeopardy with requirement 4 of CIP-004. This would result in non-compliance with two standards for a single infraction.</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>
<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>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>		
MRO's NERC Standards Review Subcommittee	Yes	The clarifications made in R6 regarding the definition of “Remote Access” were a large improvement over previous revisions.
<p>Response: Thank you for your comments.</p>		
Kansas City Power & Light	No	<p>The intent and spirit of the changes are generally beneficial and the proposed revisions provide much needed clarity regarding expected minimums. There are some clarifications and typographical errors that should be resolved prior to final approval.</p> <p>The remote access definition probably should state “or” instead of “and” for the activities and remove the monitoring reference. “used for support or maintenance, which originates from”. The second paragraph in</p>

Organization	Yes or No	Question 2 Comment
		<p>the remote access definition has an extra “t” by “purpose of CIP-005-4 Requirements.” Protection considerations should address those instances where remote access can alter or change cyber function. Monitoring should not be included.</p> <p>R6.3.3 appears to be missing at least two commas which disrupts the structure of the requirement. It should read: “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. “ The additions are noted with “, <>“.</p> <p>R6.5 may be difficult to create a policy around or to enforce. The RE would be compelled to apply restrictions on Cyber Assets outside of its direct control. RE Cyber Assets for remote access are likely to be connected infrequently, which will complicate patching and anti-malware signature updates. Cyber Assets from vendors or consultants do not utilize the RE at all in these areas, which will make verification of patch levels and anti-malware signatures next to impossible. If the RE uses brand ABC anti-malware software but the vendor uses brand XYZ, then it will not be possible to verify signature levels. The alternative is to require a proxy system outside of the ESP that is first connected to prior to connecting to the proxy system associated with the ESP and CCAs. This second proxy system may present an undue financial or maintenance burden upon the RE.</p> <p>R6.4.2 has a potentially onerous component to it. Tracking logout / disconnect time will present significant technical and / or procedural challenges. The logical place to track remote connections is at the access point. Login time can be established based upon the time of authentication at the access point. Ideally, logout time should also be tracked at the access point to provide consistent records management. However, most access points do not have a deterministic means to technically identify logout time. The device is aware of network traffic flowing across the boundary but is not aware of the traffic’s state. Absence of traffic is not necessarily an indicator of a session having ended. A long running session may have little to no traffic at various points in time. Some remote access technologies incorporate a keep-alive signal in order to keep otherwise idle sessions active. Declaring logout time based upon lack of traffic flow or preset timeouts provides nothing more accurate than guessing at the time. Procedurally relying upon the remote user to de-authenticate at the access point is equally problematic due to human nature. The Responsible Entity will be exposed to potential violations when there was no real security risk present. The remote user could have closed the session and disconnected, but if they forgot to de-authenticate then the RE will be in violation of their policy.</p> <p>R6.1 is currently a logical impossibility and prevents remote access. If the phrase “except for the intermediate device or proxy system” were added to the latter part of the statement, it would work. So R6.1 should read: “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) except for the intermediate device or proxy system within an Electronic Security Perimeter.”Simply put, remote access is interactive access across the ESP. Effectively, the proxy system must be some form of cyber asset. If the proxy system is not excluded from the</p>

Organization	Yes or No	Question 2 Comment
		<p>requirement then the remote cyber assets do not have a system they can connect to within the ESP. If the remote CA and proxy are both outside of the ESP then the proxy effectively becomes the remote CA and is still excluded from network access into the ESP. If the proxy is within the ESP, direct network access to it is prohibited based upon the current language of the requirement.</p> <p>The intent may have been to place the proxy system within a DMZ. The DMZ and proxy system must still be placed within the ESP based upon the given definitions. Explicitly requiring a DMZ may not be an appropriate requirement given the diversity of REs affected. As written, the proposed R6.1 requirement may have unintended collateral effects in conjunction with 005-R1 requirements and in particular 005-R1.5. Otherwise secure configurations may be excluded by these unintended effects and connections.</p>
<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), and clarified in response to this and other comments, and in response to technical limitation arguments concerning logout time.</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. 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>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>Regarding Requirement R6.1, the SDT has modified the definition of remote access to remove the logical impossibility described in your comment.</p>		
Seattle City Light	No	<p>Comments: R6.5 would require a signed user agreement for remote access users. 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. 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.</p> <p>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</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
		<p>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.)</p>
<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>		
Tampa Electric	No	<p>R6: Monitoring, support and maintenance will not be the only reasons for remote interactive access. What if an non-cca application resides in the ESP, but must be accessed by users from outside of the ESP? An example might be a local card key application that sits inside the ESP but is accessed by security guards from a central monitoring station which is external to the ESP. It is recommended that this requirement allows for operation of non-cca within the ESP.</p> <p>R6.1 This requirement should allow for technical feasibility.</p> <p>R6.2: This requirement is not technically feasible for most equipment operating in a control system environment today including Remote Terminal Units (RTUs), and Programmable Logic Controllers, (PLCs). This equipment generally will not support encryption to the “host” level. In addition, issues such as latency and performance will need to be considered within control systems networks. Encryption of communication inside the access point may also obviate network-level intrusion detection controls that many entities have implemented. As it relates to requirement R6.4 it would appear that the “intermediate device” would be the only “remote node” allowed to access “hosts” within the Electronic Security Perimeter. Additionally, rather than use the term “host” (which we believe is new to the standards) the existing term “cyber asset” should be used.</p> <p>R6.4.1: I think we should provide examples of what qualifies as “multi-factor” authentication and be careful that we are not precluding any technologies that may be equivalent</p> <p>R6.4.2 This requirement is redundant to the requirement and sub-requirements of CIP005 R3. CIP005 already requires the monitoring of access to the ESP at all access points, and calls for alerting which is over and above what is proposed by the updated standard.</p>
<p>Response: Thank you for your comments. The existing set of CIP Standards requires that all Cyber Assets within an Electronic Security Perimeter must be</p>		

Organization	Yes or No	Question 2 Comment
		<p>afforded the same protections. The SDT believes that this principle is appropriately applied to remote access. The term “Cyber Asset” is used in the standard; the term “host” is only used in the guidance document.</p> <p>Requirement R6 applies to access for support and maintenance, not operational access as described in the comment.</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), and clarified in response to this and other comments, and in response to technical limitation arguments.</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 technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p>
<p>Electric Reliability Council of Texas, Inc.</p>	<p>No</p>	<p>In addition to the comments submitted in response to question 1, ERCOT ISO offers the following recommendations. ERCOT ISO requests revision to the definition of remote access. “Remote access for the purpose of this standard means the ability for a person to log in to a computer or network within an organization from an external network not under the Responsible Entity’s administrative control.” ERCOT ISO requests that the term “proxy system” be removed from R6.1. This is redundant and not necessary.</p> <p>Regarding the Severe VSL, ERCOT ISO requests:</p> <ol style="list-style-type: none"> 1) Revise the wording to match the language of the requirement, “failed to 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 an the Electronic Security Perimeter.” 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>”ERCOT ISO requests the following change to Measure 6.</p> <p>M6. The responsible Entity shall make available documentation of the remote access controls as specified in Requirement R6. This is limited to the acceptable use policy and signed user agreements pursuant to Requirement R6.5.</p>
<p>Response: Thank you for your comments.</p> <p>We have created a new local definition for “intermediate device” and have included the phrase “proxy system” as part of that new definition.</p> <p>The VSLs have been modified to reflect the revised requirements language, and are consistent with existing VSL language and format.</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
<p>Measurement M6 has been modified to reflect changes made to Requirement R6.</p>		
PacifiCorp	No	<p>See previous answer. The presence of updated anti-virus software and the application of the latest security patches do not guarantee a secure workstation. Thus, a responsible entity cannot trust the security of an individual workstation. Furthermore, there is little, if any, reliability benefit that can be derived from vendor or contractor assurances that they are adhering to secure practices without validation. As such, from the perspective of a responsible entity, there is no mechanism by which the entity can actually demonstrate that any third parties follow any agreement governing remote access. Consequently, the proposed revisions merely add overhead to the responsible entity without a significant reliability benefit.</p>
<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>		
Arizona Public Service Company	No	<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> <ol style="list-style-type: none"> 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. 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 the purpose or nature of the access. 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. 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.

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
		<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 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 it 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</p>		

Organization	Yes or No	Question 2 Comment
<p>added to the associated guidance document which addresses how the connection requirements can be met.</p>		
<p>Georgia System Operations Corp & Georgia Transmission Corp</p>	<p>No</p>	<p>(1)In the proposed definition for “remote access,” it refers to remote access as “user interactive access by a person, used for monitoring, support, and maintenance.” The standard then goes on to define “support and maintenance” but does not define monitoring. This is problematic due to the discussion of “real-time monitoring” as a use case on page 8 of the draft guidance document. The guidance document introduces a new concept for “monitoring” that is not consistent with the terms use in other areas of CIP-005-4 [CIP-005-4 R1.5, R1.6, R2.2, R3, R3.1, R3.2, and R6.4.2]. If the drafting team meant the reader to infer the description of “monitoring” identified in the guidance document use case and not the more commonly understood meaning of the term used elsewhere in the standard, then the drafting team should be more deliberate in its approach. Perhaps the drafting team should be less prescriptive in its definition of remote access. GTC and GSOC recommend the CIP-005 working group refer to the industry comments received on the “BES Cyber System Maintenance” requirements of CIP-011 which indicated that remote access should not be defined by its purpose. By limiting the definition of remote access to only those functions listed as well as those covered by CAN-005, there is the potential for remote access to be granted without adequate protection. GTC and GSOC recommend the following alternative definition: “Remote access, for the purpose of CIP-005-4 Requirement R6 and its subrequirements, is user interactive access by a person to a Critical Cyber Asset, for purposes other than controlling Bulk Electric System assets from System Operator laptops, which originates from a Cyber Asset not located within any of the Responsible Entity’s Electronic Security Perimeter(s). Remote access can be initiated from:</p> <ol style="list-style-type: none"> 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” <p>(2)GTC and GSOC request that the CIP-005 working group clarify that their intent in R6.3.1 was for a Responsible Entity to individually authorize its personnel and authorize its vendor remote access by company name and not by individual. Further, GTC and GSOC request that the CIP-005 working group clarify this intent in R6.3.2 through the following change: “Maintain a record of all individuals and vendors authorized for remote access and review these records in accordance with CIP-004-4 Requirement R4.” This important clarification should allow entities the flexibility to grant vendors access for remote support in urgent situations where the specific vendor support individual is not known in advance.</p> <p>(3)GTC and GSOC are concerned with how R6.5 may be audited. While we agree that this is an important policy consideration, we are concerned with the amount and level of evidence that may be required in order to prove that an entity and all of its vendors are operating in accordance with this policy in every case. Additionally, GTC and GSOC are concerned with the language of R6.5. Specifically we refer the CIP-005</p>

Organization	Yes or No	Question 2 Comment
		<p>working group to FERC Order 706 paragraph 75 where the Commission directed the ERO to include appropriate implementation language in CIP Reliability Standards.</p> <p>(4) Consistent with CIP-004 R2 and R3, GTC and GSOC request that the CIP-005 working group add language to R6.5.4 which allows for Responsible Entities to grant remote access in emergency circumstances without first obtaining a signed acknowledgement of the remote access policy. Specifically, GTC and GSOC recommend the following modification: “R6.5.4. Signed and dated acknowledgement of the remote access user agreement by all remote access users except in specified circumstances such as an emergency. “</p> <p>(5)GTC and GSOC urge the CIP-005 working group to reconsider its position on technical feasibility exceptions. There is no known “intermediate” device to effectively implement this standard in a substation environment. While one could easily use the examples given in a scenario where remote access took place between a corporate headquarters and a substation, this does not consider the full extent of the remote access definition. The following case has not been given adequate consideration: access to an IP connected protective relay from outside the ESP by a laptop that is inside the substation where the protective relay is located. This is defined as “remote access” per the definition because it originates from outside the substation ESP. While an entity could conceivably implement a centrally located “intermediate device,” this does not allow access to the protective relay when communications to the substation are down. While there are substation data concentrators that could potentially meet this requirement, the functions that they perform would dictate that they be located within the ESP and therefore could not also function as an intermediate device outside of the ESP.</p>
<p>Response: Thank you for your comments. The definitions have been modified in response to this and other comments.</p> <p>The work of this SDT will be carried forward to the Project 2008-06 SDT for their consideration.</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 SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment. 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>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>		

Organization	Yes or No	Question 2 Comment
NextEra Energy	No	<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 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.</p> <p>Requirement R6.2.3 should be reworded to embed the frequency, as such: “Annually assess that the technical controls for Remote Access are implemented as authorized and remediate any findings.”For</p> <p>Requirement R6.3, NextEra Energy recommends defining Multifactor Control in the NERC Glossary. 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 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. 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> <p>NextEra Energy proposes the rewording of requirement R6.4.3 to read, “Implement, and document the</p>

Organization	Yes or No	Question 2 Comment
		<p>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>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 Electronic Security Perimeter. If the initiating Cyber Asset is within any of the Responsible Entity’s Electronic Security Perimeters, 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 Electronic Security Perimeter 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 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>		

Organization	Yes or No	Question 2 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>
Southern Company Transmission	No	<p>While many of the revisions are helpful, more work is needed. Please consider the following:</p> <p>R6 and local definitions</p> <ul style="list-style-type: none"> • The definition of "remote access" in R6 says that remote access can be initiated from cyber assets that are "owned" by the responsible entity, employees, contractors, vendors, or consultants. This should be struck from the definition as basing this on "ownership" is problematic. Is a leased machine "owned" by an entity? How does one prove ownership of a device before allowing it to connect? Ownership is not auditable. The standard should focus on the technical controls necessary for the remote access (as it does in R6.5) and not pull ownership into audits. • The definition of remote access includes "monitoring, support, and maintenance". It goes on to provide a definition of "support and maintenance" but does not address monitoring. Monitoring could easily get confused with "system operator laptops" that have been addressed in a previous CAN as CCA's, as these laptops 'monitor' the BES. Does monitoring include 'view only' stations from which no control can be initiated? These types of 'remote access' are left in an ambiguous state with these definitions. <p>R6.1</p> <ul style="list-style-type: none"> • The term 'direct network access' is ambiguous and undefined and it is the basis of the requirement, thus it is what would have to be proven in an audit. Need more definition to avoid audit surprises in the future. • The requirement that the intermediary access host be located inside an ESP is not sufficiently clearly spelled out within the wording of the standard but relies on the supporting documentation. • The requirement that the intermediary access host be located inside an ESP is overly prescriptive; there is no clear technical argument to be made that this is a superior element, so it should be left to the discretion of the RE. <p>R6.2</p> <ul style="list-style-type: none"> • What does "a network outside the control of the Responsible Entity" mean? Is a leased frame relay circuit from a public carrier within our control or not? The heart of the matter is whether the network segment is dedicated to an entity or shared and should be reworded to address this.

Organization	Yes or No	Question 2 Comment
		<p>R6.3.3</p> <ul style="list-style-type: none"> • This should be moved to become R6.4.3. R6.3 concerns procedural controls and R6.4 addresses technical controls. This requirement for annual assessment of technical controls should be a sub-requirement of the technical controls requirement. • R6.3.3 also contains grammatical errors. <p>R6.4.1</p> <ul style="list-style-type: none"> • Needs the language added so that TFE's could be requested. There may be situations where two factor authentication cannot be used. • Does not define multifactor authentication or provide any guidance as to what is considered acceptable to meet the requirement. <p>R6.5</p> <ul style="list-style-type: none"> • Is an administrative control with no counterpart anywhere else in the body of the NERC standards; this should be implemented as a technical control if the technology is available. Since it's not at this time, the requirement should be deleted, since it's a workload generator with no benefit to actual security. <p>R6.5.4</p> <ul style="list-style-type: none"> • The requirement to have a signed agreement from all remote access users is onerous. It is ok for employees, but the requirement should allow agreements between entities (such as the utility and its control system vendor) that cover all the vendor's users, not at an individual user level. As written, it would require every vendor or contractor employee to sign an individual agreement with every utility. • R6.5.1 through R6.5.3 should be bullet points under R6.5 and not individual sub-requirements in order to make it clear that the documentation of a policy addressing these points is the issue. As separate sub-requirements, it could be taken to mean that the utility has to provide evidence that every machine that remotely connects has updated malware signatures and updated patches for all operating systems and applications for every remote access. Device level information should not be the intent of these requirements.
<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>The technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p> <p>Requirement 6.1 has been updated based on this and other comments. The definition of Interactive remote Access has been modified to specify that</p>		

Organization	Yes or No	Question 2 Comment
<p>communications from the intermediate device to devices within the Electronic Security Perimeter is not considered interactive remote access.</p> <p>Requirement 6.2 has been updated based on this comment to address shared vs. dedicated communications.</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 list in Requirement R6.5 has been changed to an enumerated list. In NERC Standards, enumerated lists are used when each element on the list must be accomplished in order to meet the requirement; bulleted lists are used when the Responsible Entity can choose which elements of the list to implement.</p>		
Northeast Utilities	No	<ol style="list-style-type: none"> 1) The missing Canadian nuclear exclusion should be reinstated 2) Associated guidance document should have an explicit disclaimer that auditors cannot audit to this associated document 3) Request clarification of 6.2. What is the "Cyber Asset performing remote access"? The maintenance machine or the Cyber Asset being connected? 4) Recommend removing R6.3.1 and R6.3.2 because of the double jeopardy with CIP-004 R4 5) Recommend changing R6.4 from “technical controls” to “controls” to allow procedural controls 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>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</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
<p>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>		
Manitoba Hydro	No	<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"</p>
<p>Response: Thank you for your comments. The SDT believes that dial-up access meets the proposed definition of Remote Access. The guidance document has been updated to reflect this.</p>		
US Army Corps of Engineers - Omaha District	No	<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>		
Great River Energy	No	<p>Requirement 6.4.1 should include the words 'where technically feasible'. There are perimeter protection technologies that do not support two-factor authentication. By not allowing a TFE for certain multi-factor authentication technologies will lead to a degradation in reliability.</p>
<p>Response: Thank you for your comments.</p> <p>The technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
Consultant	No	<p>These added requirements are not separate from the existing requirement R2, but rather, and only in part, an amplification of that requirement. A more appropriate title for R2 might be "Remote Electronic Access Controls", because that is actually the subject of the existing sub-requirements of R2. Attempting to create this separation of requirements as indicated in this draft is confusing at best. Also, several items in the added requirement R6 & sub-requirements are redundant to existing requirements of the CIP standards.</p> <p>The "new" sub-requirement R6.3 is redundant to the provisions of the existing requirement R5, Access Control, currently contained in CIP-003. The "new" sub-requirement R6.4.2 is redundant to the requirement R3, Monitoring Electronic Access in this standard.</p> <p>The "new" sub-requirement R6.5 is inappropriate, and does not add to the security of the protected assets. This is comparable to asserting that if an agreement is signed and documented that the individual has not had any criminal history for the last seven years is equivalent to actually performing a background check. The Responsible Entity may have contractual remedies for individuals, vendors, or contractors that do not maintain their equipment to these conditions, and may even be a "best practice", but from a regulatory requirement perspective, this is merely an exercise in paper creation with no added value to the security of the protected cyber assets.</p> <p>While there may be a perception that the remote electronic access controls and monitoring requirements should be enhanced from what previously existing in sub-requirement R2.5 of CIP-005-3, those changes should be made in the context of the existing requirements. This is NOT a new requirement, and the changes as written obfuscate the issue rather than clarifying what requirements are appropriate for remote electronic access control and monitoring.</p>
<p>Response: Thank you for your comments. Requirement R2 deals with establishing the access control point on the Electronic Security Perimeter, while R6 deals with "remote access" as defined within the requirement.</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.</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>		
PNM Resources	No	<p>Definition of Remote Access</p> <p>The definition of remote access appears too vague and would benefit from language to clarify intent. The definition uses the phrase "used for monitoring, support, and maintenance." With the use of the conjunction</p>

Organization	Yes or No	Question 2 Comment
		<p>word “and” it appears that all three activities must be purpose of the remote access for the remote access restrictions to apply. If a remote access was only used for support and maintenance then falls into a regulatory void with no restrictions or guidance to Registered Entities. Use of the terms “monitoring, support and maintenance” may create ambiguity. It appears as though the intent would be “monitoring, or support and maintenance,…” The SDT should define if any, all, or combination of the three activities need to be perform to met the definition of remote access. The use of “monitoring” in the definition now may require inclusion of access to read-only access utilized by a user. This appears to represent a new concept not previously included in remote access requirements. The absence of a definition for monitoring could include a wide variety of assets including: monitoring BES telemetry, monitoring disk space on a cyber asset within or on the perimeter of the ESP, or monitoring system performance logs. Some of these tasks would fall in support and maintenance activities. We recommend clarification of the context of monitoring, or removal of the term from the requirements.</p> <p>In addition the remote access definition has no clear destination qualification. Thus any user interactive access occurring outside any Responsible Entities ESP would meet this definition. The definition should include “which originates from a Cyber Asset not located within any of the Responsible Entity’s Electronic Security Perimeters, transmitted via an intermediate device or proxy system, with a destination of a cyber asset within, or on the perimeter of, any of the Responsible Entity’s Electronic Security Perimeter.” The remote access definition should not rely on the subsequent definition of support and maintenance for destination qualification. In addition because monitoring is not subsequently defined, and if it is revised so only one of the activities need to be perform, then there is no destination qualification for monitoring.</p> <p>Also the qualification of origin of remote access is separate from the definition statement. If this limitation is intended to be applicable then it should be within the requirement language, not the definition. We would recommend insertion of these items as subrequirements of R6.4 if they are required.</p> <p>R6</p> <p>The statement for R6 needs to be reworded due to the fact that it states “shall first”. Many Responsible Entities have already implemented remote access, so “first” may create confusion. Also, the higher level requirement do not include the verbs “establish and document” although they are used in the subrequirements. Suggested wording would be,</p> <p style="padding-left: 40px;">A Responsible Entity allowing remote access to Cyber Asset within, or on the perimeter, of its Electronic Security Perimeter(s) shall establish, implement, and document the controls in the following subrequirements:</p> <p>R6.1</p> <p>R6.1 does not have any wording indicating the Responsible Entity must document the intermediate or proxy</p>

Organization	Yes or No	Question 2 Comment
		<p>system. However without documentation a Responsible Entity cannot successfully defend and audit. In addition, the term network access is vague. The requirement should use either previously used wording of routable or actually invoke the OSI layer model in the requirement. Suggested wording is,</p> <p style="padding-left: 40px;">Implement, and document an intermediate device or proxy system such that the Cyber Asset performing remote access does not have direct routable, or OSI layer three, access to Cyber Asset(s) within the Electronic Security Perimeter.</p> <p>R6.2</p> <p>R6.2 doesn't not have any wording indicating the Responsible Entity must document the implementation required. Again the standard should start with "Implement, and document". In addition the requirement should state "and the intermediate device or proxy system are encrypted." Requirement 6.1 stated both any references should to those systems should employ both or replace 'intermediate device or proxy system' with a NERC definition and update the NERC glossary.</p> <p>R6.3</p> <p>R6.3 The phrase "controls for access authorization of remote access" needs clarity. It is not clear if the requirement is referring to authorization of remote access or just remote access.</p> <p>R6.3.3</p> <p>R6.3.3. Recommend inclusion at R6.x requirement level, not subrequirement level. It may also benefit from rewording. Suggested wording is,</p> <p style="padding-left: 40px;">Establish, implement, and document a procedure to 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>R6.4.1</p> <p>While multifactor authentication should be used for some forms of remote access, it may not be appropriate for others. For example, the definition of remote access opens requirements to any read-only (monitoring) access. A proxy system could provide read-only access to information pushed to it from a cyber asset within an ESP. The connection to the proxy server may not necessitate multifactor, as it may be protection for FERC code of conduct information protection only. Requirement R6.1 requires uses of a proxy system or intermediate device. It is unclear where this multifactor authentication must now occur. Is it between the intermediate device or proxy system and the cyber asset within or on the perimeter of the ESP? Or is it between the intermediate device or proxy system and the cyber asset performing remote access? This needs</p>

Organization	Yes or No	Question 2 Comment
		<p>to be clarified. In addition since remote access includes monitoring a scenario is possible where a historian exists on the corporate network, and it gets pushed originating from cyber asset within the ESP. An engineer logs on to the historian to view the data. This could constitute remote access for a monitoring activity. The historian could be considered to be the proxy system. It in this common configuration it is not clear how multifactor authentication must be implemented. The information on the historian already has to be protected for code of conduct purposes. It is not reasonable to require multifactor authentication between the historian and the cyber asset within the ESP since the cyber asset perform a push. It is not reasonable to have to require multifactor authentication just for data residing on a historian. Thus multifactor should not be required for read-only access. The definition of remote access also has no destination qualification. If the destination qualification was like the one used in our comments on the definition of remote access, then this kind of scenario would not even qualify for remote access consideration as the interactive access really had a destination of the proxy system, not at a cyber asset within, or on the perimeter of an ESP.</p> <p>R6.4.2</p> <p>For requirement 6.4.2, destination qualification is necessary for definition of remote access to properly understand this requirement.</p> <p>R6.5</p> <p>While these requirements are generally used as best practices for remote access, they may not be necessary because of the requirement R6.1. The use of an intermediate device or proxy system could mitigate the propagation of a virus from the cyber asset performing remote access to the cyber asset within, or on the perimeter of the ESP. Especially, if the intermediate device or proxy system allows an application layer connection such as SSL VPN, or RDP then this vector would not allow for viruses to propagate to inside ESP. Requirements R6.5.1 through R6.5.3 are best practices when remote access is through a direct VPN from a remote device to another device or network. Requirement R6.1 doesn't allow for this, thus these requirements may not add additional clarity. It appears as though none of the R6.5.x requirements address where the protections must be implemented. Does R6.5.1 or R6.5.2 need to be on the intermediate device, or proxy system, or the cyber asset performing the remote access or both? Does R6.5.3 need to be between the intermediate device or proxy system and cyber asset within or on the perimeter of the ESP, or the cyber asset performing remote access and the intermediate device and proxy system? We recommend removal of the R6.5 requirement.</p>
<p>Response: Thank you for your comments. The definitions have been modified based on this and other comments. The phrase “shall first” has been removed from the requirement.</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
		<p>Requirement R6 specifies that the Responsible Entity must "...establish, document, implement and maintain the controls in the following subrequirements:" It is not necessary to specify a requirement to "document" each implementation in each of the subrequirements. Each Responsible Entity must be able to demonstrate to an auditor that the requirement has been met. Documentation of an implementation is one method to accomplish this.</p> <p>For 6.1, Requirement R6 requires "establish, document, implement and maintain" the sub-requirements. R6.1 and R6.2 are not procedural in nature, therefore documentation is not necessary. A requirement specifies what needs to be done. Demonstrating that that requirement has been met is not part of the requirement itself; it is part of the measurement. 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), and clarified in response to this and other comments, and in response to technical limitation arguments.</p> <p>The technical feasibility exception language has been added for multi-factor authentication and for dial-up encryption.</p> <p>The Drafting Team believes that "read-only" access can still be compromised to induce errors or to further compromise Critical Cyber Assets based on network connectivity.</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>
Dynergy Inc.	Yes	
NIPSCO	No	<p>The modifications proposed in CIP-005-4 create a number of issues without scoping and defining terms appropriately. Issues in regards to remote access, VPN termination point, system to system non-interactive communication, and the approved approach for authentication. In addition we have concerns over the treatment of the intermediary device that is being required by the standards. As the device is being required within the CIP standards, an entity could assume that the intermediary device should be treated as an associated cyber asset and therefore subject to the CIP standards itself. If the intermediary device was subject to the CIP standards, then an entity would need to place the device within an ESP and in turn, in order to access the device the entity would need to implement yet another intermediary device, and so on... In addition, we have concerns regarding the additional language requiring entities to navigate through the intermediary device in order to manage the ESP itself. In some entity network configurations this would require the use of a less trusted asset to manage a critical cyber asset. Finally, we are concerned that the additional language conflicts with the language provided in the recent CAN regarding remote access.</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</p>		

Organization	Yes or No	Question 2 Comment
<p>R6 has been deleted to remove ambiguity surrounding the status of the intermediary device.</p> <p>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>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>Kansas City Power & Light</p>	<p>No</p>	<p>The intent and spirit of the changes are generally beneficial and the proposed revisions provide much needed clarity regarding expected minimums.</p> <p>There are some clarifications and typographical errors that should be resolved prior to final approval.</p> <p>R6.3.3 appears to be missing at least two commas which disrupts the structure of the requirement. It should read: “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. “ The additions are noted with “, <>“</p> <p>R6.4.2 has a potentially onerous component to it. Tracking logout / disconnect time will present significant technical and / or procedural challenges. The logical place to track remote connections is at the access point. Login time can be established based upon the time of authentication at the access point. Ideally, logout time should also be tracked at the access point to provide consistent records management.</p> <p>However, most access points do not have a deterministic means to technically identify logout time. The device is aware of network traffic flowing across the boundary but is not aware of the traffic’s state. Absence of traffic is not necessarily an indicator of a session having ended. A long running session may have little to no traffic at various points in time. Some remote access technologies incorporate a keep-alive signal in order to keep otherwise idle sessions active. Declaring logout time based upon lack of traffic flow or preset timeouts provides nothing more accurate than guessing at the time.</p> <p>Procedurally relying upon the remote user to de-authenticate at the access point is equally problematic due to human nature. The Responsible Entity will be exposed to potential violations when there was no real security risk present. The remote user could have closed the session and disconnected, but if they forgot to de-authenticate then the RE will be in violation of their policy.</p> <p>R6.1 is currently a logical impossibility and prevents remote access. If the phrase “except for the intermediate device or proxy system” were added to the latter part of the statement, it would work. So R6.1 should read: “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) except for the intermediate device or proxy system within an Electronic Security Perimeter.”Simply put, remote access is interactive access across the ESP. Effectively, the proxy system must be some form of cyber asset. If the proxy system is not excluded from the requirement then the remote cyber assets do not have a system they can connect to within the ESP. If the</p>

Organization	Yes or No	Question 2 Comment
		<p>remote CA and proxy are both outside of the ESP then the proxy effectively becomes the remote CA and is still excluded from network access into the ESP. If the proxy is within the ESP, direct network access to it is prohibited based upon the current language of the requirement.</p> <p>The intent may have been to place the proxy system within a DMZ. The DMZ and proxy system must still be placed within the ESP based upon the given definitions. Explicitly requiring a DMZ may not be an appropriate requirement given the diversity of REs affected.</p>
<p>Response: Thank you for your comments. The typographical errors have been corrected.</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), and clarified in response to this and other comments, and in response to technical limitation arguments.</p> <p>Regarding Requirement R6.1, The SDT has modified the definition of remote access to remove the logical impossibility described in your comment. The SDT has also added a new local definition for intermediate device to address how the device is classified and protected in a particular environment.</p>		
MidAmerican Energy Company	No	<p>Overall the proposed revisions create additional undefined terms, prescribe “how” not “what” and introduce confusing redundancy/overlap to other existing standards. Existing R2.4 and R2.5 should be enhanced minimally to achieve the desired result.</p> <p>Improvements could instead focus on a requirement that the entity have a program that defines protections based on the protocols (interactive and non-interactive) that are allowed in and out of the ESP. Requiring a program provides more flexibility to match protections to protocol risks than the proposed “one-size” prescriptive list. Note: The guideline document is a resource for entities in tailoring and designing their program.</p> <p>If prescriptive changes as drafted proceed, the following should be changed.</p> <p>The proposed revisions delete the existing R2.4 and create a separate R6. This is problematic. The concepts of R2.4 for interactive access into the ESP still fit in context with R2. Creating a new requirement at the end creates confusion with requirements that were not changed. If a new “R” is created, it would be better placed in R2 or after R2 (in which case existing R3-R5 would be moved down and renumbered.) Make it clear that none of proposed R6 applies to dial up.</p> <p>Additionally, the existing R2.5 includes remote accesses. Draft R6.3.1 and .2 overlap and create confusion with existing R2.5.1 and 2.5.3 (draft R2.4.1 and R2.4.3). It would be better to add clarity in the existing R, not create more confusion with duplicative Rs.”Cyber Asset” is used problematically in the R6.1, R6.2, and R6.5 the definition. In the existing standards, “Cyber Asset” applies only to assets inside ESPs, except in specific circumstances called out in CIP-005 R1.5 (ESP access control and/or monitoring) and CIP-006 (PSP authorize and/or log) which maybe outside an ESP.</p>

Organization	Yes or No	Question 2 Comment
		<p>R6.1: Are the jump servers created in draft R6.1 also subject to existing R1.5?</p> <p>R6.1 and R6.2: In draft R6.1 and R6.2, replace “Cyber Asset performing” with “device initiating.”</p> <p>R6.5: Overall, R6.5 should be deleted (see below) which resolves the problem with “Cyber Asset” the draft. The measures prescribed in R6.1 and R6.2, as well as other existing measures in other requirements in the standards, eliminates the need for measures in R6.5 for the initiating device, with the exception of the prohibition of VPN split tunneling. Prohibiting VPN split tunneling is a better fit with draft R6.1 requirements for a jump server. As drafted R6.5 introduces administration that technologically cannot be enforced.</p> <p>Definition: In the first paragraph, replace all reference to “Cyber Asset” with “device.” R6.3.3, if needed, fits better in existing CIP-005-3 R4 as part of the annual vulnerability assessment. R6.1: Replace “or” with “and/or” -- Implement an intermediate device AND/OR proxy system. Depending on the protocols, an entity may have a combination. For example, some protocols may require an intermediate device. Other protocols may be controlled by a proxy at a firewall capable of proxy.</p> <p>The proposed VSLs are documentation focused. If a new requirement is created, its VSLs should be implementation and results focused. Overall, VSLs will better support reliability if they are structured to address FERC’s keys to effective compliance: prevention, detect/cease/report, mitigate/correct. VSLs should reflect if a documented program has been implemented (prevent), there is active monitoring of the program (detect/cease/report), and a corrective actions program is active (mitigate/correct).</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.

The language of original Requirement R2.4 specifically deals with “external interactive access”, which is now contained in R6. Original requirement R2.5 deals with all external accesses, interactive or not, and therefore still applies there.

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.

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.

In requirement R6.1, we agree with your comment to add “initiating” and made updates accordingly.

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

Organization	Yes or No	Question 2 Comment
		<p>added to the associated guidance document which addresses how the connection requirements can be met.</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. 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>The VSLs have been modified to reflect the revised requirements language, and are consistent with existing VSL language and format.</p>
Duke Energy	No	<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, specifically to strike the term “monitoring” from the definition.</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>		
United Illuminating	No	<p>UI understands and concurs with the requirement to require an intermediate device or proxy system. UI has concerns though.</p> <p>UI comments that the sentence listing the Examples of cyber assets (last sentence of second paragraph) that this is applicable to should be removed. UI understands the drafting team added the sentence at the request of other commenters. The difficulty with such lists is they are not all inclusive, and may list items that are not meant to be listed. If the drafting team decides to maintain the sentence then UI suggests adding the word</p>

Organization	Yes or No	Question 2 Comment
		<p>“may include”.</p> <p>UI comments on 6.1. As stated in question 1, UI would value guidance on whether the proxy intermediate device will be considered a cyber asset controlling access and thereby subject to CIP-005 R1.5. The proxy device is not controlling access to the ESP in all implementations.</p> <p>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. 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. 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> <p>This does not represent an unanswerable challenge to the drafting team. The drafting team can recognize that in this instance there is no method to guarantee that the remote access terminal is updated with all patches and is being utilized in a safe manner. In fact, the use of the intermediate proxy is required specifically to aid in relieving this risk. An organization with critical cyber assets must treat all remote access connections as suspect. UI restates that the appropriate security approach is to distrust any and all remote access connections.</p>
<p>Response: Thank you for your comments. The definitions have been modified based on this and other 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. 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>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>		
Entergy Services	No	<p>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.</p>

Organization	Yes or No	Question 2 Comment
<p>Response: Thank you for your comments. The definition of “interactive remote access” has been updated to address this issue.</p>		
<p>Exelon</p>	<p>No</p>	<p>: The following sections require clarification or revision.</p> <p>R6.1. What requirements apply to the proxy/jump server specified here? Is it an Access Control and Monitoring Asset (AMA) or is it outside the scope of CIP requirements for reporting, procedural and technical controls?</p> <p>R6.2. What requirements apply to the shared network of Energy conglomerates or holding companies that have more than one responsible entity within the corporate structure and share a common network infrastructure? Where is the boundary for required encrypted communication?</p> <p>R6.3 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.</p> <p>R6.4.1 should be clarified to exactly which access requires multi-factor authentication: The ESP or the proxy/jump server?</p> <p>R6.5 should be eliminated as it provides no technical benefit to ensure that remote access endpoints will be secure. The awareness training should be covered in the annual training required in CIP-004 R2.2.</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, and to indicate where multi-factor authentication is required.</p> <p>Requirement R6.2 has been modified to allow “corporate affiliate” networks to be used without requiring encryption.</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</p>		

Organization	Yes or No	Question 2 Comment
<p>added to the associated guidance document which addresses how the connection requirements can be met.</p>		
BGE	No	<p>- 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 entit</p>
<p>Response: Thank you for your comments. The definitions have been modified based on this and other comments.</p>		
CenterPoint Energy	No	<p>CenterPoint Energy does not agree with the proposed revisions. (See Comments to Q1 above). Overall, CenterPoint Energy views the changes to CIP-005-3 as overly prescriptive and believes the current CIP-005-3 provides an adequate mandatory level of security. As stated above, Responsible Entities are free to enhance remote access controls over and above the requirements. With the mandating of multiple controls the SDT appears to be intent on forcing all Responsible Entities that opt to provide for remote access to take a “gold plated” approach to remote access security.</p> <p>CenterPoint Energy recommends that the requirement be structured similar to CIP-006 R4 where several security (physical) options are provided. An intermediate device or proxy system, encryption, and multifactor authentication are all good examples of remote access controls; however, Responsible Entities should have more flexibility to implement one or more of the controls as most appropriate for their respective environments.</p> <p>CenterPoint Energy appreciates the apparent consideration of comments previously submitted; however, CenterPoint Energy does not fully agree with all proposed revisions to the CIP-005-3 and recommends the following:</p> <p>R6 -- Revisions note 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.” Therefore, contractors are listed twice. CNP suggests that “contractors” be removed from (2).</p> <p>R6.1 -- CenterPoint Energy recommends that the Standard Drafting Team (SDT) clarify that the intermediate device or proxy system is not considered a remote access point to the ESP and will not be subject to the CIP remote access control requirements.</p> <p>R6.3.1 -- CenterPoint Energy recommends that R6.3.1 be revised to read as follows:”Restrict remote access to authorized individuals.”This change makes the language/terms similar to what is used in other requirements and removes the need to identify groups of people from which some valid groups may be omitted. (See R6.3.2)</p> <p>R6.3.3 and R6.4.2 -- CenterPoint Energy suggests that R6.3.3 and R6.4.2 be switched since R6.3 addresses</p>

Organization	Yes or No	Question 2 Comment
		<p>procedural controls and R6.4 addresses technical controls.</p> <p>R6.4.2 -- CenterPoint Energy recommends that R6.4.2 be modified to replace “monitoring” with “reviewing” as monitoring indicates a different meaning and resulting action to be taken.</p> <p>R6.5 -- CenterPoint Energy strongly recommends that R6.5 be deleted as the remote access requirements will be covered in the Cyber Security Policy upon the implementation of these changes to the CIP Standards. (See CIP-002 R.1.1) Additionally, a separate remote access policy does not materially enhance security since there is not a feasible way to enforce the policy without impacting the timeliness of operational fixes and the reliability of the Bulk Electric System.</p> <p>Alternatively, if the SDT still perceives a need to require a separate written policy as a component of remote access security, CenterPoint Energy would like to highlight a concern about possible methods to test or demonstrate compliance to the requirement as written.</p> <p>M6 leaves much room for interpretation of what evidence would be sufficient in a Compliance Audit. Following the pattern of other standards/requirements involving a policy, an appropriate measure would read as follows: “The Responsible Entity shall make available documentation of its remote access user policy as specified in Requirement R6.” (See also CIP-003, Measure, M1.)</p> <p>Also, R6.5.4 should be removed as it references a signed and dated remote access agreement that was in a prior version of changes.</p> <p>CenterPoint Energy also recommends that the Violation Severity Levels be revised to read as follows:</p> <p>Lower - The Responsible Entity elected to allow remote access to Cyber Assets within its Electronic Security Perimeter(s) and failed to implement one of the sub-requirements of R6 (R6.1, R6.2, R6.3, R6.4, or R6.5).</p> <p>Moderate - The Responsible Entity elected to allow remote access to Cyber Assets within its Electronic Security Perimeter(s) and failed to implement two of the sub-requirements of R6 (R6.1, R6.2, R6.3, R6.4, or R6.5).</p> <p>High - The Responsible Entity elected to allow remote access to Cyber Assets within its Electronic Security Perimeter(s) and failed to implement three of the sub-requirements of R6 (R6.1, R6.2, R6.3, R6.4, or R6.5).</p> <p>Severe - The Responsible Entity elected to allow remote access to Cyber Assets within its Electronic Security Perimeter(s) and failed to successfully implement four or more of the sub-requirements of R6 (R6.1, R6.2, R6.3, R6.4, or R6.5).</p>
<p>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)”. The US Government expressed concern over insecure remote</p>		

Organization	Yes or No	Question 2 Comment
		<p>access configurations as expressed in that bulletin; therefore, requirements concerning remote access are necessary.</p> <p>The definitions have been modified based on this and other 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, and to indicate where multi-factor authentication 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. Measurement M6 has been modified to reflect changes made to Requirement R6.</p> <p>The VSLs have been modified to reflect the revised requirements language, and are consistent with existing VSL language and format.</p>
American Electric Power	No	<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</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
		"whitelisting" style applications that do not require signature updates.
<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. 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> <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>		
FirstEnergy	No	Please refer to FE's concurrent ballot comments
<p>Response: Thank you for your comments. Please refer to our responses in the ballot comment document.</p>		
Wisconsin Electric Power Company d/b/a We Energies	Yes	
PPL Electric Utilities	No	<p>PPL EU would like to thank the SDT for addressing many of the comments provided during the September commenting period. Although PPL EU agrees with and support many of the proposed revisions, PPL EU would like to see clarification on the following points:</p> <p>R 6 -- Note in box - Remove ' or contractors' from the second phrase Cyber Assets owned by employees or contractors'</p> <p>R 6.1 -- Is CIP-005 R6.1 or the Secure Remote Guidelines document requiring that the new intermediate device or proxy system be considered an access point, a Critical Cyber Asset, reside in an ESP, or that the device be subject to any NERC Standards and Requirements other than CIP-005 R6? The Secure Remote Guidelines document states on page 20 that the 'jump host computer ... in a DMZ and the DMZ is an ESP ... but does not hold any Critical Cyber Assets, just covered assets (Cyber Assets used for authentication and monitoring.' PPL EU is concerned that although authentication is performed at the ESP firewall, the standard</p>

Organization	Yes or No	Question 2 Comment
		<p>and/or the Guideline document is requiring the new device be considered a cyber asset used in access control and monitoring of the ESP; and therefore, subject to other NERC Standards as opposed to the ESP firewall being the cyber asset used in access control and monitoring of the ESP. Please clarify classification of the new devices.</p> <p>R6.3.1 Revise language ‘ ... to authorized individuals.’ as opposed to ‘authorized Responsible Entity personnel and vendors.’ as the current language is not consistent with R6 employees, contractors, vendors, or consultants.</p> <p>R 6.4 -- Revise language ‘... to prevent unauthorized individuals from establishing remote access.’</p> <p>R 6.5.3 -- Is “split-tunneling” prohibited in all designs, or is “split-tunneling” only prohibited when connecting to multiple networks where 1 or more are not under the Responsible Entity’s control?</p> <p>R 6.5.4 -- Is it the intent of the SDT to have each individual user sign a user agreement, or to have a contractor company sign a user agreement for the contractor workers at the Responsible Entity?</p>
<p>Response: Thank you for your comments. The definitions have been modified in response to this and other 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>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 “split-tunneling” and “dual homed” portions of R6.5 have been split into separate statements to reduce the confusion.</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>		
American Transmission Company	No	<p>ATC has several concerns with the changes made to the Standard and requests that the SDT address our comments prior to issuing the final draft of CIP-005.</p> <p>Requirement R6.1. states “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 an Electronic Security Perimeter.”</p> <p>There is confusion throughout the industry on this requirement regarding the appropriate classification of the intermediate device or proxy. Based on how its function is interpreted, it could be classified as a non-covered cyber asset, a component of the ESP, or a CCA which would have to be brought inside the ESP defeating its</p>

Organization	Yes or No	Question 2 Comment
		<p>intended function. Additional clarity needs to be provided by the SDT.</p> <ul style="list-style-type: none"> o R6.3.1: states “Restrict remote access to authorized Responsible Entity personnel and vendors”. ATC believes this is inconsistent with the “gray rationale box” presented in the redline version next to Requirement 6 which calls out remote access by “vendors, contractors, and consultants. ATC suggests consistent identification of parties who can initiate a remote access session. <p>Furthermore, R6 Gray Rationale box includes several examples of support and maintenance activities, none of which appear to be routine troubleshooting and problem resolution to keep the Cyber Asset functioning. ATC suggests adding troubleshooting to the maintenance example.</p> <ul style="list-style-type: none"> o Regarding Requirement R6.5, it is not clear how the policy requiring non-employee remote users to do the following: update their device’s anti-malware software and signatures; update application patches; and prohibiting use of “dual-homed” workstations or “split-tunneling” will be monitored and enforced. ATC suggests this requirement be deleted until a process for effective monitoring can be communicated. o R6.5.3. currently states “Prohibition of VPN “split-tunneling” and “dual-homed” workstations which can concurrently access multiple networks.” ATC believes the risk of split-tunneling and dual-homed workstations is, if they were to access an ESP, not whether they can access multiple networks. ATC suggests the following language: “Prohibition of VPN “split-tunneling” and “dual-homed” workstations for remote access to a designated ESP.”
<p>Response: Thank you for your comments. “Troubleshooting” has been added to the list of examples in the definition.</p> <p>The term “performing” has been removed from Requirement 6.2.</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> <p>The “split-tunneling” and “dual homed” portions of R6.5 have been split into separate statements to reduce the confusion.</p>		
Ameren	No	<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

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
		<p>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.</p> <ul style="list-style-type: none"> • 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 Electronic Security Perimeter, and all other Cyber Assets. Since the standards do not place any other requirements on Cyber Assets not within an Electronic Security Perimeter, all Cyber Assets not located within an Electronic Security Perimeter 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>		
National Grid	No	R2.3 and R2.4 should be removed and the corresponding text related to dial-up access should be moved 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>Response: Thank you for your comments. Dial-up access is not restricted to “interactive remote access”, and is sometimes used for operational (e.g., telemetry) purposes. Since Requirement R2 deals with the establishment of the Electronic SecurityPerimeter, it is appropriate for dial-up to be referenced in Requirement R2 as well as Requirement R6.</p>		
Georgia Transmission Corporation	No	GTC supports the comments submitted by Georgia System Operations Corporation.

Organization	Yes or No	Question 2 Comment
<p>Response: Thank you for your comments. Please refer to our responses to the Georgia System Operations Corporation comments.</p>		
<p>ISO New England</p>	<p>No</p>	<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. 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. 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 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>Midwest ISO</p>	<p>No</p>	<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> <p>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-</p>

Organization	Yes or No	Question 2 Comment
		<p>requirements.</p> <p>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.</p> <p>3. R6.3.2 is duplicative to CIP-004-3 R4. If the standards drafting team 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-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</p>

Organization	Yes or No	Question 2 Comment
		<p>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), and clarified 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>		
Oncor Electric Delivery	No	<p>Request revision to the definition of remote access. “Remote access for the purpose of this standard means the ability for a person to log in to a computer or network within an organization from an external network not under the Responsible Entity’s administrative control.” Requests that the term “proxy system” be removed from R6.1. This is redundant and not necessary.</p> <p>Regarding the Severe VSL:</p> <ol style="list-style-type: none"> 1) Revise the wording to match the language of the requirement, “failed to 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 an the Electronic Security Perimeter.” 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>”Request the following change to Measure 6.</p>

Organization	Yes or No	Question 2 Comment
		<p>M6. The responsible Entity shall make available documentation of the remote access controls as specified in Requirement R6. This is limited to the acceptable use policy and signed user agreements pursuant to Requirement R6.5.</p>
<p>Response: Thank you for your comments. The definitions have been modified in response to this and other comments. The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment. The term “performing” has been removed from Requirement 6.2. The VSLs have been modified to reflect the revised requirements language, and are consistent with existing VSL language and format. Measurement M6 has been modified to reflect changes made to Requirement R6.</p>		
<p>New York Independent System Operator</p>	<p>No</p>	<p>The NYISO generally agrees with the proposed revisions to CIP-005-3; however, we feel the following changes are needed in order for the NYISO to submit a “yes” vote on the draft standard:</p> <ul style="list-style-type: none"> • R6.1 -- Recommend that the language be revised to clarify that the intermediate device must be outside the ESP, or possibly in parallel with the ESP access point. • R6.3, R6.3.1, and R6.3.2 should be removed because they are redundant with CIP-004 R4 and thus create a “double jeopardy” situation in which one mistake could potentially result in non-compliance with multiple requirements. • R6.4 - Recommend changing from “technical controls” to “controls” to allow procedural controls for 6.4.2. • R6.5 -- Recommend removing R6.5 because it is redundant with existing processes required by CIP-004 and because the intermediate device required by R6.1 is a superior mitigating control compared with the proposed R6.5.
<p>Response: Thank you for your comments. The SDT has added a new local definition for intermediate device to address how the device is classified and protected in a particular environment. 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. 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</p>		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 2 Comment
<p>added to the associated guidance document which addresses how the connection requirements can be met.</p>		
WECC	No	<p>We agree with the majority of the proposed revisions but provide the following for consideration</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 offering no protection, and yet the responsible entity would be able to argue that they met the requirement. 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 …” 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. The Drafting Team has changed the encryption language in Requirement R6.2.</p> <p>The Drafting Team does not believe that the proposed change (“protected by encryption”) adds significantly to the requirement, and may in fact raise additional questions for interpretation (i.e., protect to what level). A section on encryption has been added to the associated guideline.</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>		
Independent Electricity System Operator	No	<p>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. The associated guidance document Secure Remote Access--Draft should have an explicit disclaimer that it will not be used for audit purposes. In our comments to the first draft of CIP-005-4 we expressed concern that an entity that violates Requirement R6 could also be found non-compliant with R2 since R6 has replaced and expanded on the now deleted R2.4. It does not appear to us that this concern has been addressed in the Consideration of Comments to the previous posting.</p> <p>In R6.2 the "Cyber Asset performing remote access" must be clarified. Is it the maintenance machine, or the</p>

Organization	Yes or No	Question 2 Comment
		<p>Cyber Asset being connected?</p> <p>Because of the double jeopardy with CIP-004 R4 we recommend replacing R6.3.1 and R6.3.2 with the following text: “Restrict remote access to persons identified pursuant to CIP-004-4 Requirement R4. Change the wording in R6.4 from “technical controls” to “controls” to allow for procedural controls.</p> <p>VRFs and VSLs (for R6)</p> <ul style="list-style-type: none"> • All VSLs -- In the part of the VSL that refers to sub-requirement 6.5, replace “acceptable use policy” with “remote access use policy” to match the wording of the requirement. The phrase “acceptable use policy” appears only in the SAR. • Moderate VSL -- Conforming changes to the first part must be made based on our proposed change to the requirement. • High VSL -- Delete the first part based on our proposed change to the requirements. In the second part delete “technical” as per our comments. • Severe VSL -- The text of the first and second parts should reflect the wording of the requirements. Specifically “remote Cyber Asset” does not appear in R6.1 and R6.2 while clarification of "Cyber Asset performing remote access" has been requested; and “public network” does not appear in R6.2 only in the SAR. <p>Editorial comments</p> <ul style="list-style-type: none"> • In the Purpose statement, “CIP-009-3” should be “CIP-009-4”. • In R1.5, second line, delete “a” before “specified” • In the text box on page 3, second paragraph, delete “t” before “CIP-005-4” • For consistency with the current format of the standard, all references to “Parts” of requirements should be to “Sub-requirements”. <p>Finally, the document identified on the project web page as “Redline to Last Approved -- Revised 12/01-10” is actually a redline to the last posted... sort of. The changes from the approved version of CIP-005-3 have all been accepted. Also the second paragraph in the Effective Date section should be redlined in this version since it is new. Stakeholders may overlook changes that are not redlined.</p> <p>Similarly, the posted Draft SAR Version 1 contains changes that have not been redlined.</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>		

Organization	Yes or No	Question 2 Comment
		<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. 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>Numerous editorial changes and correction of typographical errors have been made.</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 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 VSLs have been modified to reflect the revised requirements language, and are consistent with existing VSL language and format.</p>
Portland General Electric Company	Yes	<p>(1) The language in the grey box next to Requirement 6 needs to be incorporated into the text of Requirement 6 so that the standard is clear and uncluttered.</p> <p>(2) The proposed revisions to this standard create a new class of assets, "intermediate device or proxy system." However, it is not clear what controls are intended to apply to devices that fall into this new category.</p> <p>(3) It is not clear what equipment is meant by "Cyber Assets used to initiate remote access" in Requirement 6.5.</p>
<p>Response: Thank you for your comments. The language in the gray box is a local definition, which will remain with 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.</p> <p>Regarding R6.5, the equipment to be addressed is that equipment which is used to perform the functions described in the definition of “interactive remote access”</p>		

3. Do you agree with the proposed implementation language (six months to comply with the new Requirement R6 after the standard becomes effective)?

Summary Consideration:

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.

Organization	Yes or No	Question 3 Comment
Northeast Power Coordinating Council	Yes	
Bonneville Power Administration	No	BPA does not believe that 6 months provides enough time. Even assuming that our comment regarding remote access is accepted, 6 months is insufficient time to comply with the requirement in an appropriate manner.
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.		
Electric Market Policy	No	Dominion would be able to vote yes if the issues identified in the proposed revisions to CIP-005-3 are addressed.
Response: Thank you for your comments.		
Hydro One Networks	Yes	
MRO's NERC Standards Review Subcommittee	No	If an entity has remote substations designated as Critical Assets, 6 months does not provide ample time for research into technologies, re-design of the substation automation networks, and installation and testing. If this were only applied to EMS/SCADA systems at control centers, 6 months would be adequate. However, when entities are faced with long travel routes to and from remote substations, and that same travel is again required for troubleshooting, 6 months does not provide a reasonable implementation period for the new requirements placed on entities in R6 (installation of proxy servers, remote access systems, and new access controls). Recommend 18 months. Reasons for additional lead time would be to get asset ordered and budget approvals, installation of the asset, and to make sure the asset meets CIP requirements.

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
<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>		
Kansas City Power & Light	No	This could take some up to 12 months to implement and test.
<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>		
Seattle City Light	No	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. The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>		
Tampa Electric	No	We recommend any changes agreed upon by NERC should follow the CIP Version 4 implementation plan.
<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>		
Electric Reliability Council of Texas, Inc.	No	As these new requirements may result in significant changes to infrastructure for some organizations, request a longer implementation period than six months from effective date. Implementation of new infrastructure may have significant cost that has not been identified for 2011 budgeting. Other entities may have to increase 24x7 on-site support to address issues that arise. Funding of these efforts may require that funds be diverted from other reliability-related efforts if adequate implementation time is not allowed.
<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>		
PacifiCorp	No	PacifiCorp believes that, if Requirement R6 is ultimately in effect to govern responsible entities’ remote access controls, a six-month timetable for complete implementation would be insufficient because it fails to reflect the third-party arrangements that are implicated by these controls. It may be the case that implementing and enforcing security requirements upon responsible entity-owned cyber assets is perhaps workable in 12 months. However, it will take longer than 12 months to establish the contractual obligations for remote support vendors and perform the legal reviews concerning the rights and obligations of a responsible entity within existing contracts, not including the timeframes for implementation and enforcement.

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
<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>		
Arizona Public Service Company	Yes	
Georgia System Operations Corp & Georgia Transmission Corp	No	<p>GTC and GSOC do not agree with the proposed implementation language. GTC and GSOC recommend that the effective date of CIP-005-4 be aligned with the other version 4 CIP standards (8 calendar quarters following applicable regulatory approval) to prevent a staggered version 4 implementation timeline. Additionally, it is unclear what the difference is in requiring compliance six months after the effective date versus requiring an effective date of five calendar quarters following applicable regulatory approval. The additional wording regarding implementation appears to be unnecessary.</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>		
NextEra Energy	No	<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 Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently approved by industry.</p>		
Southern Company Transmission	No	<p>For larger systems, six months is not a sufficient timeframe for implementation. Propose 12 months for implementation with the opportunity for extension for defined assets for good cause and approved by the regional entity.</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>		
Northeast Utilities	No	<p>Suggest changing from six months to twelve months to comply</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>		
Manitoba Hydro	No	<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>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
<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> <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>		
US Army Corps of Engineers - Omaha District	Yes	
Great River Energy	Yes	
Consultant	No	<p>The requirements R6.1, R6.2, and R6.4.1 may require procurement and installation of hardware and software that may not be available within six months of the effective date of the standard. There needs to be a provision to allow delays where procurement and installation of equipment cannot be completed in this implementation time frame.</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>		
PNM Resources	No	<p>Because compliance to the revision may necessitate implementation of technical controls, a compliance timeline of 12 months would be more appropriate to allow sufficient time for testing and implementation.</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>		
Dynergy Inc.	Yes	
NIPSCO	No	<p>The proposed implementation plan conflicts with the implementation plan for CIP-002-4. CIP-002-4 defines a list of Cyber Assets and Critical Cyber Assets that for some entities that may differ dramatically from version 3 of the standards. The version 3 assets will be subject to the newly modified requirements of CIP-005-4 and later the list of impacted Critical Cyber Assets may change based on the delayed effective date of CIP-002-4. The effective dates for this set of standards need to be aligned to avoid; unnecessary critical network modifications, unnecessary network redesign, and unnecessary associated capital and O&M expenses for a</p>

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
		temporary compliance effort that will change for a number of entities when CIP-002-4 becomes effective.
<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>		
Kansas City Power & Light		
MidAmerican Energy Company	No	The time required to implement procedures and perform training to achieve compliance would exceed the six month deadline in Requirement R6.
<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>		
Duke Energy	Yes	
United Illuminating	Yes	
Entergy Services	Yes	
Exelon	No	The six month compliance period may prove too short for full implementation of these changes, particularly where projects in-progress will have to change implementation to meet these requirements. Suggest that a one-year implementation period would be more appropriate for the complexity of changes required by this revision, and to allow adequate time for project extensions or revisions to meet the new requirements.
<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>		
BGE	No	BGE disagrees with an implementation plan of 6 months. BGE believes that a 12-month implementation period for the new Requirement R6 after the standard becomes effective is needed.
<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>		
CenterPoint Energy	Yes	CenterPoint Energy agrees with the proposed implementation language.

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
Response: Thank you for your comments.		
American Electric Power	No	Depending upon the consideration of our comments, purchasing and implementing enterprise-wide hardware solutions can take much more time than six months after implementation.
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.		
FirstEnergy	Yes	
Wisconsin Electric Power Company d/b/a We Energies	No	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.
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.		
PPL Electric Utilities	Yes	
American Transmission Company	No	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, ATC is very concerned as to how the policy would be monitored and enforced. These issues require at least a 12 month implementation period.
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.		
Ameren	Yes	
National Grid	No	National Grid recommends having “one year” to comply with the new requirement R6 after the standard becomes effective.
Response: Thank you for your comments. The Drafting Team has modified the implementation timeframe to be consistent with the “Version 4” standards recently		

Consideration of Comments on Urgent Action Revisions to CIP-005-3— Project 2010-15

Organization	Yes or No	Question 3 Comment
approved by industry.		
Georgia Transmission Corporation	No	GTC supports the comments submitted by Georgia System Operations Corporation.
Response: Thank you for your comments. Please see the SDT responses to Georgia System operations Center’s comments.		
ISO New England	Yes	
Midwest ISO		
Oncor Electric Delivery	No	As these new requirements may result in significant changes to infrastructure for some organizations, request a longer implementation period than six months from effective date. Implementation of new infrastructure may have significant cost that has not been identified for 2011 budgeting. Other entities may have to increase 24x7 on-site support to address issues that arise. Funding of these efforts may require that funds be diverted from other reliability-related efforts if adequate implementation time is not allowed.
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.		
New York Independent System Operator	Yes	
WECC		
Independent Electricity System Operator	Yes	
Portland General Electric Company	Yes	

END OF REPORT