NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Consideration of Comments

Interpretation 2012-INT-04
CIP-007 for ITC

The Interpretation 2012-INT-04 Drafting Team thanks all commenters who submitted comments on the Interpretation of CIP-007-3, Requirement R5, for ITC (Project 2012-INT-04). This interpretation was posted for a 30-day public comment period from November 9, 2012 through December 10, 2012. Stakeholders were asked to provide feedback on the interpretation and associated documents through a special electronic comment form. There were 31 sets of comments, including comments from approximately 95 different people from approximately 60 companies representing 9 of the 10 Industry Segments as shown in the table on the following pages.

All comments submitted may be reviewed in their original format on the standard's project page.

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, Mark Lauby, at 404-446-2560 or at mark.lauby@nerc.net. In addition, there is a NERC Reliability Standards Appeals Process.[1]

[1] The appeals process is in the Standard Processes Manual: http://www.nerc.com/files/Appendix_3A_StandardsProcessesManual_20120131.pdf

Index to Questions, Comments, and Responses

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										X

	Additional Member	Additional Organization	Region	Segment Selection
1.	Alan Adamson	New York State Reliability Council, LLC	NPCC	10
2.	Carmen Agavriloai	Independent Electricity System Operator	NPCC	2
3.	Greg Campoli	New York 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.	Mike Garton	Dominion Resources Services, Inc.	NPCC	5
8.	Kathleen Goodman	ISO - New England	NPCC	2
9.	Michael Jones	National Grid	NPCC	1
10.	David Kiguel	Hydro One Networks Inc.	NPCC	1

Group/Individual	Commenter	Organization	Registered Ballot Body Segment									
			1	2	3	4	5	6	7	8	9	10

11.	Christina Koncz	PSEG Power LLC	NPCC	5
12.	Randy MacDonald	New Brunswick Power Transmission	NPCC	9
13.	Bruce Metruck	New York Power Authority	NPCC	6
14.	Silvia Parada Mitchell	NextEra Energy, LLC	NPCC	5
15.	Lee Pedowicz	Northeast Power Coordinating Council	NPCC	10
16.	Robert Pellegrini	The United Illuminating Company	NPCC	1
17.	Si-Truc Phan	Hydro-Quebec TransEnergie	NPCC	1
18.	David Ramkalawan	Ontario Power Generation, Inc.	NPCC	5
19.	Brian Robinson	Utility Services	NPCC	8
20.	Brian Shanahan	National Grid	NPCC	1
21.	Wayne Sipperly	New York Power Authority	NPCC	5
22.	Donald Weaver	New Brunswick System Operator	NPCC	2
23.	Ben Wu	Orange and Rockland Utilities	NPCC	1
24.	Peter Yost	Consolidated Edison Co. of New York, Inc.	NPCC	3

2.	Group	Trey Cross	ACES COOP Members	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	East Kentucky Power Cooperative		SERC	1, 3, 5, 6
2.	Arizona Electric Power Cooperative, Inc.		WECC	5, 6
3.	Southwest Transmission Cooperative		WECC	1
4.	Brazos Electric Power Co Op, Inc.			1, 3, 5

3.	Group	Sasa Maljukan	Hydro One Networks Inc.	X									

	Additional Member	Additional Organization	Region	Segment Selection
1.	David KIGUEL	Hydro One Networks Inc.	NPCC	1
2.	Kim GROSSKURTH	Hydro One Networks Inc.	NPCC	1
3.	Jason SNAGGS	Hydro One Networks Inc.	NPCC	1

4.	Group	Chris Higgins	Bonneville Power Administration	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Forrest Krigbaum	System Operations	WECC	1
2.	Huy Ngo	Control Cntr HW Design & Maint	WECC	1
3.	Thomas Gist	CC HW Dsgn/Stds Montr & Admin	WECC	1
4.	Mark Tucker	FERC Compliance	WECC	1, 3, 5, 6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
5.	Group	Greg Goodrich	ISO/RTO Council Security Working Group		X								

	Additional Member	Additional Organization	Region	Segment Selection
1.	Steve McElew	PJM	RFC	2
2.	Ann Delenela	ERCOT	ERCOT	2
3.	Lesley Bingham	SPP	SPP	2
4.	Jeff Norek	AESO	WECC	2
5.	Peter Kramp	MISO	RFC	2
6.	Tim Lockwood	CAISO	WECC	2
7.	John Galloway	ISO-NE	NPCC	2

6.	Group	Connie Lowe	Dominion	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Greg Dodson		SERC	1, 3, 5, 6
2.	Randi Heise		MRO	5, 6
3.	Mike Garton		NPCC	5, 6
4.	Louis Slade		RFC	5, 6

7.	Group	David Dockery	Associated Electric Cooperative, Inc. - JRO00088	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Central Electric Power Cooperative		SERC	1, 3
2.	KAMO Electric Cooperative		SERC	1, 3
3.	M & A Electric Power Cooperative		SERC	1, 3
4.	Northeast Missouri Electric Power Cooperative		SERC	1, 3
5.	N.W. Electric Power Cooperative, Inc.		SERC	1, 3
6.	Sho-Me Power Electric Cooperative		SERC	1, 3

8.	Group	Larry Raczkowski	FirstEnergy Corp	X		X	X	X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	William J Smith	FirstEnergy Corp	RFC	1
2.	Steve Kern	FirstEnergy Energy Delivery	RFC	3
3.	Doug Hohlbaugh	Ohio Edison	RFC	4
4.	Ken Dresner	FirstEnergy Solutions	RFC	5
5.	Kevin Querry	FirstEnergy Solutions	RFC	6

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
9.	Group	Greg Rowland	Duke Energy	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Doug Hils	Duke Energy	RFC	1
2.	Lee Schuster	Duke Energy	FRCC	3
3.	Dale Goodwine	Duke Energy	SERC	5
4.	Greg Cecil	Duke Energy	RFC	6

10.	Group	Brent Ingebrigtson	PPL NERC Registered Affiliates	X		X		X	X				

	Additional Member	Additional Organization	Region	Segment Selection
1.	Brenda Truhe	PPL Electric Utilities Corporation	RFC	1
2.	Annetee Bannon	PPL Generation LLC on behalf of Supply NERC Registered Affiliates	RFC	5
3.			WECC	5
4.	Elizabeth Davis	PPL Energy Plus LLC	MRO	6
5.			NPCC	6
6.			SERC	6
7.			SPP	6
8.			RFC	6
9.			WECC	6

11.	Group	Emily Pennel	Southwest Power Pool Regional Entity										X
No additional members listed.													
12.	Individual	Shane Eaker	Southern Company	X		X		X	X				
13.	Individual	James Gower	Entergy	X		X		X					
14.	Individual	Bob Steiger	Salt River Project	X		X		X	X				
15.	Individual	Thad Ness	American Electric Power	X		X		X	X				
16.	Individual	Nazra Gladu	Manitoba Hydro	X		X		X	X				
17.	Individual	Cade James Simmons	MidAmerican Energy Company	X		X		X					
18.	Individual	Michael Falvo	Independent Electricity System Operator		X								
19.	Individual	Patrick Brown	Essential Power, LLC					X					
20.	Individual	Don Jones	Texas Reliability Entity										X
21.	Individual	Randi Nyholm	Minnesota Power	X									

Group/Individual		Commenter	Organization	Registered Ballot Body Segment									
				1	2	3	4	5	6	7	8	9	10
22.	Individual	Shari Heino	Brazos Electric Power Cooperative, Inc.	X				X					
23.	Individual	Bill Fowler	City of Tallahassee	X		X		X					
24.	Individual	Michael R. Lombardi	Northeast Utilities	X		X		X					
25.	Individual	Brett Holland	Kansas City Power & Light	X		X		X	X				
26.	Individual	Patricia Boody	Tampa Electric Company	X		X		X	X				
27.	Individual	Anthony Jablonski	ReliabiltiyFirst										X
28.	Individual	Andrew Gallo	City of Austin dba Austin Energy	X		X	X	X	X				
29.	Individual	Michael Moltane	ITC	X									
30.	Individual	Cheryl Moseley	Electric Reliability Council of Texas, Inc.		X								
31.	Individual	David Jendras	Ameren	X		X		X	X				

IF YOU WISH TO EXPRESS SUPPORT FOR ANOTHER ENTITY'S COMMENTS WITHOUT ENTERING ANY ADDITIONAL COMMENTS, YOU MAY DO SO HERE.

Summary Consideration:

N/A

Organization	Yes or No	Do you agree with another entity's comment?
Brazos Electric Power Cooperative, Inc.		ACES Power Marketing
City of Austin dba Austin Energy	Agree	Electric Reliability Council of Texas, Inc. ("ERCOT").

1. **Do you agree with this interpretation's response to Question 1 (Whether each sub-requirement of Requirement R5 requires both "technical and procedural controls.")? If not, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.**

Summary Consideration:

The IDT removed the phrase "using technology" in relation to "procedural control" in response to a comment that pointed out that a procedural control itself is not required to use technology.

Some commenters also suggested that the interpretation be shorter in response to question 1, but given the background in development of this answer, on balance, the additional explanation provides clarifying rationale. The IDT did separate the response into distinct paragraphs, however.

Some commenters questioned the discussion in the interpretation regarding "implementation." The IDT discusses implementation because it believes that is a key element to the requirement that gives greater credence to the notion that it does not matter whether the control is technical or procedural, as the control must be implemented, not just be a policy in place.

Commenters raised various points regarding CAN-0017, including suggestions for modification and retirement. In reference to CAN-0017, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and the CAN is not part of the standard. However, the IDT understands that any interpretation that is contrary to the CAN will supersede the CAN. The IDT expects that any portion of the CAN that does not correspond with the interpretation will be retired or changed to conform to the approved interpretation.

A commenter suggested clarification of the standard language to read "technical or procedural controls". The IDT agrees in concept on this point, but notes that, according to the Guidelines for Interpretation Drafting Teams, an interpretation cannot change the language in the standard.

Some commenters raised specific questions on compliance, or on use of the TFE process in the language. The IDT notes in response that the interpretation specifies what is required by the language of the standard, not specific guidance or approaches for how certain entities may apply the requirements to their specific situations. Providing guidance related to TFEs is beyond the scope or authority of an interpretation drafting team.

A commenter raised a question regarding coordination between this interpretation and another request for interpretation on a similar question. The same interpretation drafting team is working on both interpretation projects (2012-INT-03 and 2012-INT-04) for consistency purposes.

In response to question one and question two, commenters raised questions regarding the IDT's discussion matrix that accompanied the unofficial comment form during the first formal comment period. The IDT developed the matrix in the background material as a means of providing additional information into the IDT's development process, and many of the examples were for illustration. It will not become part of the interpretation, and the IDT appreciates the concerns surrounding future use or reliance on the matrix. The IDT has determined that, in the best interest of clarity and to promote focus on the interpretation itself, such a matrix should no longer accompany the background material. Therefore, the IDT has removed the matrix from the comment form.

Organization	Yes or No	Question 1 Comment
American Electric Power	No	Though we agree with the overall interpretation provided to Q1, we disagree some of the insight provided. The interpretation appears to prescriptively require the use of technology within procedural controls when it states "the control is accomplished either by a human being using technology (procedural) or...". Though we agree that technology may play a role in the procedural controls utilized, we disagree with any interpretation that actually requires using technology as part of that procedural control, as this is not specified within the standard itself.
Response: The IDT agrees, and it has made clarifying changes in the response to remove "using technology" in describing the procedural control.		
Texas Reliability Entity	No	Texas RE finds the proposed Response to Question 1 to be unduly long and complicated. The answer should simply be "In R5, the reference to 'technical and procedural controls' means both technical controls and procedural controls or either one of them, as appropriate in each context." This interpretation is consistent with common and acceptable usage of the word "and" in written materials. (For the engineers, this usage corresponds to the logical OR function.)
Response: Thank you for your suggestions. The IDT understands the desire to shorten the response, but the additional explanation provides clarifying rationale. However, in response to your suggestions, the IDT has separated the response to Question 1 into two distinct paragraphs.		

Organization	Yes or No	Question 1 Comment
ReliabiltiyFirst	No	ReliabilityFirst generally agrees with the drafted question 1, CIP-007 Interpretation, but offers the following comments for consideration:The IDT does a good job of discussing the differences between technical and procedural controls, but the discussion becomes unclear when discussing the requirement for implementing each type of control. Also, the wording of the actual Interpretation is at odds with CAN-0017. CAN-0017 states "...a CEA is to verify that a registered entity has implemented the appropriate control(s) - either 1) both technical and procedural controls, or 2) only a procedural control", meaning that procedural controls are necessary for all requirements and sub-requirements, and may be supported by technical controls as appropriate. ReliabilityFirst agrees with CAN-0017 that technical controls that support procedural controls work. ReliabilityFirst does not agree that a technical control without an associated procedural control will be an effective method of implementing compliance with a requirement. ReliabilityFirst recommends the wording of the Interpretation be changed and clarified to ensure procedural controls are required for all requirements and sub-requirements to be consistent with CAN-0017.
Response: The IDT discusses implementation because it believes that is a key element to the requirement that gives greater credence to the notion that it does not matter whether the control is technical or procedural, as the control must be implemented, not just be a policy in place. In reference to CAN-0017, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams, and the CAN is not part of the standard. However, the IDT understands that any interpretation that is contrary to the CAN will supersede the CAN. The IDT expects that any portion of the CAN that does not correspond with the interpretation will be retired or changed to conform to the approved interpretation.		
Ameren	No	(1)Ameren agrees in part with the IDT interpretation; specifically we agree with the need for clarification of the suggested language change to read "technical or procedural controls". (2)We request clarification to expound on what is expected to be compliant with this requirement. Is the intent of the language change to provide situational guidance or is it to be applied

Organization	Yes or No	Question 1 Comment
		literally? In other words, will the requirement now require either a technical control or a procedural control under any circumstance, or is the requirement requiring a technical control wherever possible and procedural control when it is not feasible to use technical controls? Without clarification in the requirement language as to how and when to apply the requirement, there will be a continued opportunity for misinterpretation.(3)The interpretation should clearly indicate whether or not when a technical control is feasible it should be used and if it is not technically feasible, then a procedural control is acceptable and finally it should clarify when a TFE will be required.
Response: (1) The IDT agrees in concept on this point, but notes that, according to the Guidelines for Interpretation Drafting Teams, an interpretation cannot change the language in the standard. (2) The purpose of an interpretation is to clarify the language in the requirement, not to provide specific implementation guidance. However, the IDT notes the language requires the application of technical and procedural controls in an effort to collectively achieve compliance with the requirements and sub requirements. (3) The IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams. The IDT seeks to provide an interpretation of what is required by the language of the standard, not provide guidance or an approach of how an entity will apply the requirements to its specific situation.		
ACES COOP Members	Yes	ACES, EKPC, AEPCO and SWTC appreciate the time and analysis from the IDT in determining that R5 requires a more flexible approach to compliance by allowing for an 'Or' when an 'And' is not possible. We would also like to add this language or similar for clarification; "In the case where a specific device is capable of implementing neither a technical or procedural control, the entity would file for TFE treatment."
Response: Thank you for your support. The language being recommended provides clarity in regards to when an entity would pursue a TFE; however the standard also needs to allow for a TFE. The IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams. The IDT cannot change the language of the standard and adding the TFE applicability statement is not in scope for the IDT.		

Organization	Yes or No	Question 1 Comment
Associated Electric Cooperative, Inc. - JRO00088	Yes	AECI supports this determination and the underlying rationale.
Response: Thank you for your support.		
FirstEnergy Corp	Yes	FirstEnergy agrees it should not be necessary to implement both technical and procedural controls to comply with the sub-requirements of CIP-007 R5. We agree with the IDT view that since CAN-017 contradicts this position, it is important that CAN-0017 is retired if/when this interpretation becomes effective.
Response: Thank you for your support; this is the IDT's understanding as well.		
Duke Energy	Yes	Duke Energy agrees with the response to Question 1.
Response: Thank you for your support		
Southwest Power Pool Regional Entity	Yes	While the SPP RE agrees with the response language specific to Question 1, the SPP RE has concerns with the interpretation documentation overall. The analysis matrix should be included in the formal interpretation in some manner, subject to the following comments:The analysis matrix discussion for R5.1.2 contains what appears to be misleading guidance. After a good discussion of the need for an automated (technical) logging capability, possibly augmented with a procedural log retention control, the discussion makes reference to manually logging access to a relay via a single account. This final observation is not appropriate for R5.1.2 as the use of a single access credential by multiple relay technicians is a shared account subject to the requirements of R5.2.3. As readers of the interpretation may rely upon the analysis discussion, this aspect of the analysis needs to be corrected. Additionally, the bolded comment for R5.2.1 may need to be changed or removed. There are commercial applications available, such as

Organization	Yes or No	Question 1 Comment
		Cyber Ark, that will manage shared and administratively privileged accounts by automatically changing the passwords per an entity policy, secure those passwords in an access controlled vault, and log by individual user and date/time of access who has obtained the password for a specific system and user account. The characterization that such a capability is improbable is likely not warranted. This comment is also applicable to R5.2.3 where the discussion states that managing the use of a shared account cannot be performed by a technical control. To the contrary, utilities such as Cyber Ark are designed to do exactly that. The key is to configure the password change policy to establish a one-time-use password for each access and to control authorization via the authentication rights to the password management system and vault.
Response: Thank you for your support of the interpretation. In response to this and other comments, the IDT has determined that, in the best interest of clarity and to promote focus on the interpretation itself, such a matrix should no longer accompany the background material. Therefore, the IDT has removed the matrix from the comment form.		
Bonneville Power Administration	Yes	Bonneville Power Administration (BPA) notes that the interpretation does not give an explicit answer to Question 1. BPA strongly agrees with the statement "Therefore an entity would utilize a combination of technical and procedural controls in an effort to achieve strict compliance with the collection of requirements contained within Requirement R5, not specifically use both technical and procedural controls in achieving strict compliance for each unique sub-requirement.", and notes the following issues:First, the matrix of R5 requirements is not part of the interpretation, and should not be held as directive on Responsible Entities. BPA suggests that the sentence in the fifth paragraph of the Background ending "...understanding of the methodology used in this evaluation." be revised to "...understanding of the methodology used in this evaluation, but is not directive on the Responsible Entities." Second, the evaluation of R5.1.2 in the matrix states "A Cyber Asset must create logs with user account access

Organization	Yes or No	Question 1 Comment
		activity. Without this technical ability it would be a violation of the requirement. In this instance a TFE is not permitted."This appears to clearly deny the use of procedural controls. However, the last sentence in the evaluation of R5.1.2 explicitly allows procedural controls. BPA believes that there is no requirement that the Cyber Asset itself create logs, especially since the requirement is to produce "methods, processes, and procedures" without referring to technical controls. Finally, the evaluation of R5.3 in the matrix states "A procedure could be used to require the use of passwords." This implies that the intent of R5.3 is that all systems must use passwords, and the passwords must meet the subrequirements. It is equally valid to take R5.3 as describing the requirements that passwords must meet if passwords are used. BPA believes that the latter is the correct meaning, for several reasons. One, authentication methods such as two-factor authentication, which is much stronger than the use of passwords, would not be compliant under the first interpretation. Two, a system which allows only weak passwords might be better protected by other means such as physical access control. Three, there are legacy systems which do not have the capability to use passwords, but for which other access control methods such as physical access control can enforce adequate security.
Response: The IDT developed the matrix in the background material as a means of providing additional information into the IDT's development process, and many of the examples were for illustration. It will not become part of the interpretation, and the IDT appreciates the concerns surrounding future use or reliance on the matrix. The IDT has determined that, in the best interest of clarity and to promote focus on the interpretation itself, such a matrix no longer accompany the background material. Therefore, the IDT has removed the matrix from the comment form.		
Entergy	Yes	Entergy agrees with this interpretation of the requirements that both technical and procedural controls could be used to enforce access authentication. Where technical controls can not be implemented procedural controls will be established and implemented which require technical actions.Additionall, the latest draft of CIP version 5, states the

Organization	Yes or No	Question 1 Comment
		following in regards to passwords:For password-based user authentication, either technically or procedurally enforce the following password parameters:5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, non alphanumeric) or the maximum complexity supported by the Cyber Asset.The intent of the CIP v5 draft requirements acknowledges the limited risk to the BES by not requiring both technical and procedural controls which is consistent with Entergy's current interpretation. Entergy realizes that CAN-0017 released by NERC on November 11, 2011 is contrary to our interpretation of the requirements, however per a NERC presentation delivered on March 30, 2011, the "Purpose of CAN does not modify a reliability standard and is not a replacement for an interpretation". Currently, there is no formal NERC interpretation for this requirement.
Response: Thank you for your support and supporting comments.		
Manitoba Hydro	Yes	Manitoba Hydro recommends removal of the following statement as it adds no value to the response: "The IDT also notes that regardless of control type (technical or procedural) the entity has the compliance requirement of implementing the control and demonstrating evidence of the control." We acknowledge that the entity must show compliance to the controls deployed, as is the intention of any requirement.
Response: Thank you for your support for the interpretation, but the IDT respectfully disagrees with the suggested language removal. The IDT discusses implementation because it believes that is a key element to the requirement that gives greater credence to the notion that it does not matter whether the control is technical or procedural, as the control must be implemented, not just be a policy in place.		

Organization	Yes or No	Question 1 Comment
Northeast Utilities	Yes	NU supports this interpretation and also recommends that CAN-0017 be retired.
Response: Thank you for your support and supporting comments.		
Tampa Electric Company	Yes	Tampa Electric complements the IDT for their work in drafting this Response to the Interpretation for ITC. Tampa Electric agrees with the response to Question 1. In addition, we recommend that the IDT consider a way to include the table from the Unofficial Comments document as it provides additional clarity and information for compliance/audits. In addition, this RFI is similar to Interpretation 2012-INT-03 submitted by TECO. We recommend that the IDT address both Interpretations with the upcoming ballot. Tampa Electric requests the IDT/NERC to provide guidance to Registered Entities/Regional Entities related to TFEs that will no longer be required so that there is a uniform process across all regions. Our current options include (1) termination by the Registered Entity (2) the disapproval of a TFE by the Regional Entity. Tampa Electric recommends a termination of the TFE by the effective date of the approved RFI.
Response: The IDT developed the matrix in the background material as a means of providing additional information into the IDT's development process, and many of the examples were for illustration purposes only. In response to several comments, the IDT has determined that, in the best interest of clarity and to promote focus on the interpretation itself, such a matrix no longer accompany the background material. Therefore, the IDT has removed the matrix from the comment form. **The same interpretation drafting team is working on both interpretation projects (2012-INT-03 and 2012-INT-04) for consistency purposes.** **Providing guidance related to TFEs is beyond the scope or authority of an interpretation drafting team.**		
Hydro One Networks Inc.	Yes	

Organization	Yes or No	Question 1 Comment
ISO/RTO Council Security Working Group	Yes	
Dominion	Yes	
Southern Company	Yes	
Salt River Project	Yes	
MidAmerican Energy Company	Yes	
Independent Electricity System Operator	Yes	
Essential Power, LLC	Yes	
Minnesota Power	Yes	
Brazos Electric Power Cooperative, Inc.	Yes	
City of Tallahassee	Yes	
Kansas City Power & Light	Yes	
ITC	Yes	
Electric Reliability Council of Texas, Inc.	Yes	
Northeast Power Coordinating Council	Yes	

2. Do you agree with this interpretation's response to Question 2 (Whether technical controls in Requirement R5.3 mean that each individual Cyber Asset within the Electronic Security Perimeter (ESP) has to automatically enforce each of the three R5.3 sub-parts.)? If not, what, specifically, do you disagree with? Please provide specific suggestions or proposals for any alternative language.

Summary Consideration:

Commenters offered suggested alternatives to the final sentence in response 2, and the IDT discussed whether it would refocus the intended interpretation away from the question of the RFI. Most comments in response to question 2 were centered on the TFE language at the end of the interpretation. In response, the IDT removed reference to TFEs altogether in the response to question 2.

Commenters raised concern with the use of "strict compliance" in the interpretation. In response, the IDT clarified the use of technical and procedural concerns are for purposes of satisfying the requirement, and the IDT has removed references to "strict compliance."

Similar to question 1, some commenters raised recommendations to retire or modify CAN-0017. The IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.

A commenter suggested a change in the language of the interpretation to ensure that a technical control is implemented if it is available for a particular Cyber Asset. While this may be a preferred outcome by some, the IDT cannot change the language of the standard to provide a preference of technical over procedural.

A commenter raised a concern about a conflict in the responses to the two questions, and other commenters suggested a slight word change with respect to the automatic enforcement sentence. The IDT notes that it made several clarifying changes since the last posting, and changed "The automatic enforcement component would apply . . ." to ". . . could apply . . ."

Organization	Yes or No	Question 2 Comment
Northeast Power Coordinating Council	No	The last sentence of the response needs clarification. Recommend changing from "In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment." to "In the case where a specific device is not capable of implementing a technical control and it is not

Organization	Yes or No	Question 2 Comment
		possible to implement a procedural control on that same specific device, the entity would file for TFE treatment."
Response: The IDT considered this recommendation, but the IDT believes that it would possibly refocus the intended interpretation away from the question in the RFI, which is whether both technical and procedural controls are required by R5.3. The IDT has removed reference to TFEs in its response to question 2.		
ACES COOP Members	No	If the IDT has determined that in to be compliant with R5.3, the entity can use technical and or procedural controls, R5.3 and the sub-parts should be able to have procedural controls; if technically not possible.Thank you for the time and consideration.
Response: The IDT believes the interpretation is consistent with this comment.		
ISO/RTO Council Security Working Group	No	The ISO/RTO Council Security Working Group does not agree with the response's because the last sentence is not clear enough. The ISO/RTO SWG recommends changing from "In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment." to "In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment."
Response: The IDT considered this recommendation, but the IDT believes that it would possibly refocus the intended interpretation away from the question in the RFI, which is whether both technical and procedural controls are required by R5.3. The IDT has removed reference to TFEs in its response to question 2.		
Dominion	No	In general, Dominion agrees with the response; however, the last sentence could still be misinterpreted as requiring a TFE to be filed if only one type of control is available (technical or procedural). Dominion suggests the last sentence of the response be rewritten as follows, "A TFE should be filed if neither a technical control nor a procedural control can be implemented for requirement 5.3 or any of its individual

Organization	Yes or No	Question 2 Comment
		sub-requirements for a specific device."
Response: The IDT considered this recommendation, but the IDT believes that it would possibly refocus the intended interpretation away from the question in the RFI, which is whether both technical and procedural controls are required by R5.3. The IDT has removed reference to TFEs in its response to question 2.		
Southwest Power Pool Regional Entity	No	The interpretation asserts that the mere presence of a procedural control is sufficient to demonstrate compliance with R5.3 and its included requirements. While the standard does not prescribe the use of technical controls to assure and enforce strict compliance, the absence of such controls means that strict compliance cannot be assured. In the absence of a technical control whose configuration can be evaluated at audit, the registered entity is not able to demonstrate strict compliance short of disclosing the passwords to the auditors, something the audit teams are not willing to pursue. In effect, in the absence of auditable technical controls, this requirement is essentially not auditable and the entity cannot demonstrate compliance. Therefore, in the absence of technical controls that can be configured to enforce strict compliance, the registered entity's only recourse is to seek a Technical Feasibility Exception to provide safe harbor from a violation and apply procedural controls as the compensating and mitigating measures required by the TFE. The recommendation to retire CAN-0017 with the adoption of this interpretation is premature.
Response: The IDT clarified the use of technical and procedural concerns are for purposes of satisfying the requirement, and the IDT has removed references to "strict compliance." The IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.		
American Electric Power	No	Though we agree with the overall interpretation provided to Q2, we do not agree with the portion of the response that states "in the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment". It is not clear to us in what instance a device, by itself, could ever be considered a procedural control, as procedural controls typically occur

Organization	Yes or No	Question 2 Comment
		outside of the inherent functionality of the device.
Response: The IDT has removed reference to TFEs in its response to question 2.		
Texas Reliability Entity	No	The proposed response answers only part of Question 2. (1) Texas RE agrees that R5.3 does not have to be enforced "automatically," if that means by using only technical controls. The sub-parts of R5.3 may be enforced by procedural controls as well as by technical controls. (2) The response should make clear that ALL of the sub-parts of R5.3 are required, as technically (or procedurally)feasible. (3) Texas RE would prefer not to invite additional TFE filings in this context. If one of the sub-parts of R5.3 is not technically feasible as applied to a specific Cyber Asset, the registered entity should be prepared to demonstrate either compliance or infeasibility at the time of an audit or spot check.
Response: The IDT agrees the entity would demonstrate the procedural controls that are in place, and the IDT has also removed reference to TFEs in its response to question 2.		
Brazos Electric Power Cooperative, Inc.	No	The language is not clear. This sentence from the response to question 2 is vague because of the use of "either": "In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment." Consider rewriting it as: "In the case where a specific device is capable of implementing neither a technical nor procedural control, the entity would file for TFE treatment."
Response: The IDT has removed reference to TFEs in its response to question 2.		
ReliabiltiyFirst	No	ReliabilityFirst generally agrees with the drafted question 2 CIP-007 Interpretation, but offers the following comments for consideration:The IDT's language changes the reading of CIP-007-3 R5.3 to somewhat correspond with the wording contained in CIP-007-5 R5 Parts 5.5 and 5.6. This may ease the entities' transition into CIP Version 5 without seriously compromising security of existing systems.However, the

Organization	Yes or No	Question 2 Comment
		Interpretation needs to be clarified to ensure that technical controls for password length, complexity and age are implemented when they are available. This in enforced now by the practice of denying a TFE in the case where compliance with a requirement is “technically feasible.” If a technical control is available but not used, compliance will revert to reliance on a (presumably weaker) procedural control, which will increase risk to the BES.ReliabilityFirst recommends that the wording of the answer to Question 2 be modified to ensure that a technical control is implemented if it is available for a particular Cyber Asset.
Response: While this may be a preferred outcome by some, the IDT cannot change the language of the standard to provide a preference of technical over procedural. To reduce compliance risk and BES reliability, entities are naturally encouraged to implement technical controls vs procedural controls; however the IDT cannot make the standards language change.		
Electric Reliability Council of Texas, Inc.	No	We do not agree with this response because the response's last sentence is not clear enough. We recommend changing from " In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment. " to " In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment." ERCOT Recommendation: Recommended change to the last sentence: “In the case where a technical and/or procedural control cannot be implemented or supported for a specific device, the responsible entity is advised to request a TFE in accordance with Appendix 4D of the NERC Rules of Procedure.”
Response: The IDT has removed reference to TFEs in its response to question 2.		
Ameren	No	(1)We believe there may be a conflict between the responses for the two interpretation questions on how the requirement R5.3 should be interpreted and further clarification is requested.(a)First; the word “automatic” is not being considered as directive and is not required to achieve strict compliance and there is no mention of using the TFE process to support non-compliance. (b)Second; in

Organization	Yes or No	Question 2 Comment
		reference to “technical controls”, the word “automatic” is being treated as being directive and is required to achieve strict compliance with sub-requirements of R5.3. (2)We believe that the IDT response does not clearly indicate whether or not all Cyber Assets within an ESP must comply with the R5.3 requirements or if only the CCAs need to comply. We believe this requirement applies to all Cyber Assets with the ESP and where neither a procedural or technical control is feasible then it requires the filing of a TFE.
Response: The IDT notes that it has made several clarifying changes since the last posting of this interpretation, to include removing references to TFEs in response to question 2. In response to the concern about “automatic” being directive, the IDT has changed the language in that sentence to use the word “could” instead of “would.” The scope of the interpretation does not extend to discussion regarding applicability between CCA’s vs Cyber Assets within an ESP.		
Hydro One Networks Inc.	Yes	To improve clarity, we recommend changing last sentence from " In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment. " to " In the case where a specific device is not capable of implementing a technical control and it is not possible to implement a procedural control on that same specific device, the entity would file for TFE treatment." Also, Hydro One believes that this interpretation clarifies the issue discussed in the CAN-0017 document. Because of this we suggest NERC considers retiring it.
Response: The IDT has removed reference to TFEs in its response to question 2. The IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.		
Bonneville Power Administration	Yes	BPA notes that the Interpretation does not give an explicit answer to Question 2. BPA strongly agrees with the statement "The word automatic is absent from the language within CIP-007-3, Requirement R5, and it is therefore not required to achieve strict compliance with the individual requirements or sub-requirements.", as long as "it" refers to the use of automatic enforcement of the requirements. Also,

Organization	Yes or No	Question 2 Comment
		see comments about the matrix of R5 requirements in the comments for Question 1.
Response: Thank You for your support.		
Associated Electric Cooperative, Inc. - JRO00088	Yes	AECI supports this determination and the underlying rationale
Response: Thank you for your support.		
FirstEnergy Corp	Yes	FirstEnergy agrees that procedural controls provide an acceptable means to enforce all three sub-requirements of CIP-007 R5; technical controls should not be required. More importantly, registered entities should not be required to generate and maintain Technical Feasibility Exceptions (TFEs) when procedure controls are implemented as the sole means of enforcing these sub-requirements. Very few cyber assets provide technical controls to enforce all three sub-requirements; consequently, registered entities are currently required to generate and maintain TFEs for virtually all of their CIP cyber assets. Since these TFEs normally just document the alternate procedural controls used to enforce these requirements, these TFEs represent a tremendous administrative burden with no improvement in BES reliability.
Response: Thank you for your support.		
Duke Energy	Yes	Duke Energy agrees with the response to Question 2.
Response: Thank you for your support.		
Southern Company	Yes	Southern Company reads the IDT's response to Question 2 to state that, with respect to the context of R5.3, either technical or procedural controls may be used to demonstrate strict compliance with subrequirement R5.3 or one of its sub-subrequirements, so long as some combination of technical and procedural controls

Organization	Yes or No	Question 2 Comment
		are used to demonstrate compliance with Requirement 5 and its various subparts as a whole. In its last sentence, the IDT states that, "In the case where a specific device is not capable of implementing either a technical or procedural control, the entity would file for TFE treatment." To clarify and remove all doubt as to the reading of this phrase, Southern would suggest phrasing the last sentence in the following manner: "In the case where neither a technical nor a procedural control is capable of implementation for a specific device, the entity would file for TFE treatment with respect to R5.3 and its various subparts.
Response: IDT agrees with your reading of the IDT response. Furthermore, The IDT has removed reference to TFEs in its response to question 2.		
Manitoba Hydro	Yes	Manitoba Hydro agrees the response to Question 2 in general, but doesn't agree with the statement "The automatic enforcement component would apply to the technical controls that are implemented, ..." since it modifies the standard by adding an automatic enforcement requirement through the interpretation process, which is not allowed by the NERC Rules of Procedure. This statement should either be removed, or modified to "The automatic enforcement component could apply to the technical controls that are implemented, ..." which does not make it a strict requirement.
Response: The IDT agrees and has changed "would" to "could."		
Northeast Utilities	Yes	NU supports this interpretation and also recommends that CAN-0017 be retired.
Response: Thank you for your support. With respect to CAN-0017, the IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.		
ITC	Yes	ITC supports the results of the RFI, Interpretation 2012-ITC-04 - Interpretation of CIP-007 for ITC. However, due to long delay in this Interpretation process (~18 months since we submitted our Request for Interpretation), we have planned around this by filing a large number of Technical Feasibility Exceptions denoting

Organization	Yes or No	Question 2 Comment
		compensating/mitigating measures. We encourage NERC and the industry to continue work on development of a faster response time for Interpretation Requests to make them more useful in the future.ITC would also like to point out that since some portions of this Interpretation are in conflict with CAN-0017, that the CAN should be retired.
Response: Thank you for the support. The CIP IDT notes that it was formed specifically to address a large number or pending interpretations that had been on hold before the team was formed. It expects that future interpretations may be developed more rapidly. With respect to CAN-0017, the IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.		
Entergy	Yes	
Salt River Project	Yes	
MidAmerican Energy Company	Yes	
Independent Electricity System Operator	Yes	
Essential Power, LLC	Yes	
Minnesota Power	Yes	
City of Tallahassee	Yes	
Kansas City Power & Light	Yes	
Tampa Electric Company	Yes	

Organization	Yes or No	Question 2 Comment
PPL NERC Registered Affiliates		We agree with the interpretation, however, in support of this we believe that CAN-0017 should be revisited to address the language requiring a TFE for purely procedural controls. Specifically, number 2 in the Section "Password Controls - R5.3", currently it reads: "If a registered entity has equipment for which a technical control only partially meets the requirements of the standard, but the equipment has the capability to fulfill all the standard by implementing a procedural control for the remaining requirements, the CEA is to verify that the registered entity has implemented a procedural control for any requirements that a technical solution cannot fulfill, and has obtained, or is in the process of obtaining, a TFE." With this interpretation we believe it should be rewritten to delete the part requiring a TFE, "...the CEA is to verify that a registered entity has implemented a procedural control for any requirements that a technical solution cannot fulfill."
Response: Thank you for your support. With respect to the CAN, the IDT does not determine whether a CAN is retired or not, but it expects that the CAN, or any portion thereof, would be modified or retired in response to an approved interpretation.		

END OF REPORT