NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Consideration of Comments

## Project 2012-INT-04 Interpretation for ITC

The Project 2012-INT-04 Drafting Team thanks all commenters who submitted comments on the Interpretation of CIP-007-3, Requirement R5, for ITC. The interpretation and supporting materials were posted for a 45-day public comment period from February 6, 2013 through March 22, 2013. Stakeholders were asked to provide feedback on the interpretation and associated documents through a special electronic comment form. There were 18 sets of comments, including comments from approximately 53 different people from approximately 33 companies representing 8 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/comm/SC/Documents/Appendix_3A_StandardsProcessesManual.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 Granffenried | Consolidated Edison Co. of New York, Inc. | NPCC | 1 |
| 6. | Gerry Dunbar | Northeast Power Coordinating Council | NPCC | 10 |
| 7. | Mike Garton | Domion 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 | Dave Francis | MISO | | X | | | | | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Charles Yeung | SPP | SPP | 2 |
| 2. | Ben Li | IESO | NA - Not Applicable | 2 |
| 3. | Stephanie Monzon | PJM | RFC | 2 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3. | Group | Randi Heise | Dominion NERC Compliance Policy | X | | X | | X | X | | | | |

| | Additional Member | Additional Organization | Region | Segment Selection |
|---|---|---|---|---|
| 1. | Michael Crowley | Virginia Electric & Power Company | SERC | 1 |
| 2. | Michael Crowley | Virginia Electric & Power Company | SERC | 3 |
| 3. | Mike Garton | Dominion Energy Marketing Inc | MRO | 6 |
| 4. | Louis Slade | Dominion | MRO | 5 |
| 5. | Louis Slade | Dominion | RFC | 5 |
| 6. | Mike Garton | Dominion Energy Marketing Inc | RFC | 6 |
| 7. | Connie Lowe | Dominion | NPCC | 5 |
| 8. | Connie Lowe | Dominion Energy Marketing Inc | NPCC | 6 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4. | Group | Emily Pennel | Southwest Power Pool Regional Entity | | | | | | | | | | X |

No additional members listed.

| Group/Individual | | Commenter | Organization | Registered Ballot Body Segment | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 5. | Individual | Pamela Hunter | Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing | X | | X | | X | X | | | | |
| 6. | Individual | Shannon Fair | Colorado Springs Utilities | X | | X | | X | | | | | |
| 7. | Individual | Nazra Gladu | Manitoba Hydro | X | | X | | X | X | | | | |
| 8. | Individual | Andrew Z. Pusztai | American Transmission Company, LLC | X | | | | | | | | | |
| 9. | Individual | Michael Falvo | Independent Electricity System Operator | | X | | | | | | | | |
| 10. | Individual | John Seelke | Public Service Enterprise Group | X | | X | | X | X | | | | |
| 11. | Individual | Wryan J. Feil | Northeast Utilities | X | | | | | | | | | |
| 12. | Individual | Anthony Jablonski | ReliabilityFirst | | | | | | | | | | X |
| 13. | Individual | RoLynda Shumpert | South Carolina Electric and Gas | X | | X | | X | X | | | | |
| 14. | Individual | Brian S. Millard | Tennessee Valley Authority | X | | X | | X | X | | | | |
| 15. | Individual | Warren Cross | ACES | X | | | | X | X | | | | |
| 16. | Individual | Thad Ness | American Electric Power | X | | X | | X | X | | | | |
| 17. | Individual | Russel Mountjoy | Midwest Reliability Organization | | | | | | | | | | X |
| 18. | Individual | Brett Holland | Kansas City Power & Light | X | | X | | X | X | | | | |

**If you support the comments submitted by another entity and would like to indicate you agree with their comments, please select "agree" below and enter the entity's name in the comment section (please provide the name of the organization, trade association, group, or committee, rather than the name of the individual submitter).**

**Summary Consideration:**

**N/A**

| Organization | Agree | Supporting Comments of "Entity Name" |
|---|---|---|
| MISO | Agree | MISO, SPP, PJM |
| American Transmission Company, LLC | Agree | ATC endorses the comments submitted by MRO NSRF. |

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:**

**Several commenters questioned the use of "or" versus "and". The IDT views the impact of "technical or procedural controls" language as an implementation of either technical or procedural controls to achieve collectively the requirements within Requirement R5. The IDT recognizes the language in the parent Requirement and has provided the interpretation that supports the current language of "and".**

**There was a comment that, while the commenter agrees with the interpretation, the interpretation is in conflict with CAN-0017. In response, the IDT notes that it must interpret the language of the standard pursuant to the Guidelines for Interpretation Drafting Teams. It is important to note that an interpretation will supersede any CAN in which there is a contradiction.**

**There was a request for clarification on whether the interpretation removes the ability for an entity to submit a TFE for the sub-requirements if they are only using a procedural control. In response, after postulating instances in which some Cyber Assets are technically and procedurally incapable of meeting R5.3, the IDT notes the Responsible Entity can still file a TFE.**

**There was one commenter who stated that procedural controls should be sufficient. In response, the IDT believes this would be correct if Requirement R5 were to read "technical or procedural controls". The IDT recognizes the language in the parent Requirement and has provided the interpretation that supports the current language of "and".**

| Organization | Yes or No | Question 1 Comment |
|---|---|---|
| ReliabilityFirst | No | The IDT correctly states, "The use of 'and' in Requirement R5 indicates that the responsible entity must implement both technical and procedural controls to achieve collectively the sub-requirements within Requirement R5 and the associated sub-requirements." However, there is no basis in the language of the requirement for the following statement, "Both are not necessary for each sub-requirement individually." Had the language of the |

| Organization | Yes or No | Question 1 Comment |
|---|---|---|
| | | requirement read “technical or procedural controls,” then the IDT would have a firm basis for this statement. The result of the IDT’s Interpretation is to effectively change the language of the standard. |
| **Response: The IDT appreciates your comment, highlighting the fact that a consistent industry interpretation is necessary. In response to the comment identifying the reference of the phrase "or" versus "and", the IDT views the impact of “technical or procedural controls” language as an implementation of either technical or procedural controls to achieve collectively the requirements within Requirement R5. The implication of an “or” would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language (“and”).** | | |
| Midwest Reliability Organization | No | MRO does not support the interpretation of CIP-007-3 for ITC as presented. CIP-007-3 R5 clearly states the Responsible Entity shall establish, implement and document technical “and” procedural controls....the requirement does not offer the choice of technical “or” procedural controls, the requirement requires both through the use of “and”. |
| **Response: The IDT appreciates your comment, highlighting the fact that a consistent industry interpretation is necessary. In response to the comment identifying the reference of the phrase "or" versus "and". The IDT views the impact of “technical or procedural controls” language as an implementation of either technical or procedural controls to achieve collectively the requirements within R5. The implication of an “or” would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language (“and”).** | | |
| Colorado Springs Utilities | Yes | Colorado Springs Utilities agrees with the interpretation INT-04 CIP-007-3, but it appears to be in conflict with CAN0017. |
| **Response: 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 interpretation.** | | |

| Organization | Yes or No | Question 1 Comment |
|---|---|---|
| Public Service Enterprise Group | Yes | We support the interpretation language and have a minor request for clarification. The interpretation as is written allows either a technical and/or a procedural control to comply with the sub-requirements R5.3.x on an individual basis. Recognizing that where technically possible a device should enforce the password characteristics, does the interpretation remove the ability for an entity to submit a TFE for these sub-requirements if they are using only a procedural control? (i.e. can an entity file a TFE on password complexity and use a procedural control as one of the mitigation actions for such a TFE, or is the intent to no longer have such TFEs submitted?) |
| **Response: The IDT has postulated instances in which some Cyber Assets are technically and procedurally incapable of meeting the R5.3 requirements. In such instances, the Responsible Entity technically cannot achieve compliance with the complexity sub-requirement and so should file a TFE.** | | |
| Northeast Utilities | Yes | To meet this requirement, procedural controls should be sufficient since enforcement and training permeate through many other CIP requirements where procedural controls are sufficient. |
| **Response: The IDT appreciates your comment. In response to the comment identifying "procedural controls should be sufficient", the IDT believes this would be correct were R5 to read "technical or procedural controls". The IDT views the impact of "technical or procedural controls" language as an implementation of either technical or procedural controls to achieve collectively the requirements within R5. The implication of an "or" would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language ("and").** | | |
| South Carolina Electric and Gas | Yes | The interpretations says "...it is not necessary for both technical and procedural controls to be used in each subrequirement of Requirement R5." and I agree that it should be one or the other but not necessarily both as the word "and" implied. |

| Organization | Yes or No | Question 1 Comment |
|---|---|---|
| **Response:** The IDT appreciates your comment in support. | | |
| ACES | Yes | ACES supports the interpretation of moving from a "technical and procedural controls" to a "technical or procedural controls" understanding. |
| **Response: The IDT appreciates your comment. The IDT views the impact of "technical or procedural controls" language as an implementation of either technical or procedural controls to achieve collectively the requirements within R5. The implication of an "or" would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language ("and").** | | |
| Northeast Power Coordinating Council | Yes | |
| Dominion NERC Compliance Policy | Yes | |
| Southwest Power Pool Regional Entity | Yes | |
| Southern Company: Southern Company Services, Inc.; Alabama Power Company; Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing | Yes | |
| Independent Electricity System Operator | Yes | |
| Tennessee Valley Authority | Yes | |
| American Electric Power | Yes | |
| Kansas City Power & Light | Yes | |

| Organization | Yes or No | Question 1 Comment |
|---|---|---|
| Manitoba Hydro | | No comment. |

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:**

**There was a comment that the interpretation extends the unjustified meaning of Requirement R5 in Question 1 into the sub-requirements of Requirement R5.3. In response, the IDT views the impact of "technical or procedural controls" language as the implementation of either technical or procedural controls to achieve collectively the requirements within Requirement R5.**

**There were similar comments to Question 1 with regards to TFEs. Commenters stated that it would be helpful to include additional clarification regarding TFEs. There was a commenter who stated that entities would be ill advised if they do not seek a TFE for those instances where technical controls cannot enforce the technical password configuration requirement of the standard. In response, after postulating instances in which some Cyber Assets are technically and procedurally incapable of meeting R5.3, the IDT notes the Responsible Entity can still file a TFE.**

**There were several comments that provided clarifications or suggested revisions to the language in the sub-requirements. Pursuant to the Guidelines for Interpretation Drafting Teams, an interpretation may not be used to change an approved Reliability Standard or its applicability.**

| Organization | Yes or No | Question 2 Comment |
|---|---|---|
| ReliabilityFirst | No | The IDT extends the unjustified reading of Requirement R5 in Question 1 into the sub-requirements of Requirement R5.3. As in Question 1, there is no basis in the language of the Requirement for this reading. |
| **Response: The IDT appreciates your comment, highlighting the fact that a consistent industry interpretation is necessary. In response to the comment identifying the reference of the phrase "or" versus "and". The IDT views the impact of "technical or** | | |

| Organization | Yes or No | Question 2 Comment |
|---|---|---|
| **procedural controls" language as an implementation of either technical or procedural controls to achieve collectively the requirements within Requirement R5. The implication of an "or" would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language ("and").** | | |
| Midwest Reliability Organization | No | Technical controls providing reminders for registered entities to change passwords are necessary; however, the technical controls should not be automatically changing the passwords themselves |
| **Response: The IDT appreciates your comment, highlighting the fact that a consistent industry interpretation is necessary. In response to the comment identifying the reference of the phrase "or" versus "and". The IDT views the impact of "technical or procedural controls" language as an implementation of either technical or procedural controls to achieve collectively the requirements within R5. The implication of an "or" would allow an entity to utilize entirely procedural or entirely technical controls. The IDT recognizes the language in the parent requirement and has provided an interpretation that supports the current language ("and").** | | |
| Kansas City Power & Light | No | It would be helpful to add additional clarification regarding the TFE requirements for CIP-007-3 R5.3. A statement should be added that indicates it is possible to implement procedural controls without also requiring a TFE. There may be instances where the three R5.3 sub-parts are not automatically enforced, though procedural mechanisms are used to ensure that technically feasible password configurations or periodic activities are met. |
| **Response: The IDT has postulated instances in which some Cyber Assets are technically and procedurally incapable of meeting the R5.3 requirements. In such instances, the Responsible Entity technically cannot achieve compliance with the complexity sub-requirement and so should file a TFE.** | | |
| Southwest Power Pool Regional Entity | Yes | While the interpretation response to Question 2 is technically correct, SPP RE remains concerned that entities would be ill advised if they do not seek a Technical Feasibility Exception for those instances where technical controls cannot enforce the technical password configuration requirement of the standard. Many, but not all operating |

| Organization | Yes or No | Question 2 Comment |
|---|---|---|
| | | systems readily support the setting of a configuration control prescribing a minimum password length and a maximum password age. Most operating systems do not have the capability to prescribe a password complexity that fully meets the CIP-007-3/R5.3.2 requirement. At audit, registered entities are obligated to demonstrate compliance with the requirement. Having a procedural control, such as a password policy, instructs the user to conform but does not demonstrate that the user has actually conformed to the requirement. Compliance can be demonstrated by disclosing the password to the auditor, but that is something neither the entity nor the auditor is willing to do for cyber security reasons. That places the registered entity in a dilemma. Unless conformance can be demonstrated, compliance cannot be demonstrated and the registered entity is at risk of a possible violation. Procedural controls, along with configuring the operating system to enforce password complexity to the maximum extent possible, are good mitigating measures to support a Technical Feasibility Exception. Appendix 4D of the NERC Rules of Procedure provides for and requires a TFE for any instance where the entity cannot comply with CIP-007-3, Requirement R5 or one or more of the included requirements R5.3.1, R5.3.2, and R5.3.3. The TFE is also available and appropriate when the registered entity cannot demonstrate compliance, regardless whether actual compliance can be achieved, for the express purpose of safe harbor from a violation. The SPP RE strongly recommends the interpretation be modified to at least recommend the pursuit of a TFE in those instances where technical enforcement of the requirement is not possible. The registered entity can then make an informed decision whether to seek a TFE or risk a possible violation at audit. |
| **Response: The IDT appreciates your comment and support. According to the Guidelines for Interpretation Drafting Teams, an interpretation may not be used to change an approved Reliability Standard or its applicability.** | | |
| Northeast Utilities | Yes | However, the last sentence of the IDT interpretation needs strengthening. See the following: "The IDT interprets that the responsible entity would need to demonstrate that the [Insert word: procedural] controls have been put in place to satisfy the three |

| Organization | Yes or No | Question 2 Comment |
|---|---|---|
| | | sub-requirements of R5.3. |
| **Response: Thanks for your comment and support. However inclusion of the word "procedural" would require a change to the Standard's language. According to the Guidelines for Interpretation Drafting Teams, an interpretation may not be used to change an approved Reliability Standard or its applicability.** | | |
| Tennessee Valley Authority | Yes | TVA would like the IDT to clarify if a TFE is needed where there is a procedural control in place in the event technical enforcement is not possible. With the IDT's clarification to Question 1 that both technical and procedural controls are not necessary for each sub requirement, the argument could be made that a TFE not required when using a procedural control. |
| **Response: Thanks for your comment and support. The IDT has postulated instances in which some Cyber Assets are technically and procedurally incapable of meeting the R5.3 requirements. In such instances, the Responsible Entity technically cannot achieve compliance with the complexity sub-requirement and so should file a TFE.** | | |
| ACES | Yes | ACES supports the understanding that automatically enforcing controls is the combination of the technical and procedural controls that are implemented to satisfy the three sub-requirements of R5.3. |
| **Response: Thanks for your comment and support.** | | |
| Northeast Power Coordinating Council | Yes | |
| Dominion NERC Compliance Policy | Yes | |
| Southern Company: Southern Company Services, Inc.; Alabama Power Company; | Yes | |

| Organization | Yes or No | Question 2 Comment |
|---|---|---|
| Georgia Power Company; Gulf Power Company; Mississippi Power Company; Southern Company Generation; Southern Company Generation and Energy Marketing | | |
| Colorado Springs Utilities | Yes | |
| Independent Electricity System Operator | Yes | |
| Public Service Enterprise Group | Yes | |
| South Carolina Electric and Gas | Yes | |
| American Electric Power | Yes | |
| Manitoba Hydro | | No comment. |

END OF REPORT