Changes since video was filmed...

- Rules of Procedure Appendix 4D was simplified in Sept. 2013, but process is basically the same
- There is no longer a Part A/B – Just one submission
- We will review TFE within 60 days of request
  - We no longer accept or reject or do a Part B “deep dive” review
  - We will approve or disapprove request within 60 days
  - “Safe Harbor” begins when you request TFE
- You don’t have to complete NERC Review Worksheet (“TSAW")
- If something changes re: your Required Information, you can request changes to an approved TFE via a Material Change Form in webCDMS

December 2013
TFE Issues and Expectations

Shon Austin
Senior Compliance Specialist
saustin@spp.org · 501.614.3273
What is a TFE and when do I need one?

- **NERC Rules of Procedure Appendix 4D** allows Responsible Entity to request/receive exception from strict compliance with certain CIP Standard requirements on grounds of technical feasibility or limitations.

- TFE provides “safe harbor” from violation.
Requirements eligible for TFE

- **CIP-005-1:**
  - R2.4
  - R2.6
  - R3.1
  - R3.2

- **CIP-006-2:**
  - R1.1

- **CIP-007-1**
  - R2.3
  - R3
  - R4
  - R5.3
  - R 5.3.1
  - R 5.3.2
  - R 5.3.3
  - R6
  - R6.3
Example: CIP-006 R1

• Your control room does not have 6-wall boundary
• You submit TFE indicating **why** you aren’t in strict compliance and **how** you mitigate/compensate
• **TFE Justification:**
  – Gap at ceiling greater than 96 square inches
• **Compensating Measures – Control Room:**
  – Has 25-ft high solid concrete walls
  – Staffed 24/7
  – In access-controlled building (layered access)
SPP RE’s Expectations for Entities

1. Complete TFE request in webCDMS
   - Include justification
   - No Part A/B – Just one submission
SPP RE’s Expectations for Entities

2. Material Change: A change in facts that modifies Required Information in connection with an approved TFE.

– Examples of a Material Change could include, but are not limited to an Appendix 4D - Technical Feasibility Exception Procedure increase in device count (but not a decrease), change in compensating measures, change in statement of basis for approval for the TFE, a change in the Expiration Date of the TFE, or a Responsible Entity achieving Strict Compliance with the Applicable Requirement.
SPP RE’s review process

• Review TFE request within 60 days of TFE request
  – Approve or disapprove
  – “Safe Harbor” begins with SPP RE’s acceptance
When to amend a TFE

• Registered Entity can amend pending TFE at any time during SPP RE review
  – Must provide additional information
  – Revise required information
• Can resubmit entire TFE or only the portion being amended, if easily separable
• Approvals of amendments are at SPP RE’s discretion
Compliance Application Notice-017

- **Read CAN-0017**

- Administrator, Shared, or Other Generic Account Passwords – R5.2.1
  - Review initial password controls of default user accounts
  - Get TFE if any password controls cannot technically be met per CIP-007 R5.3 (initially or when changed)
Compliance Application Notice-017

- **Password Controls – R5.3**
- You are compliant if a technical solution is available
- **Get TFE:**
  - If you have a technical control that does not strictly comply, you must implement a procedural control to “fill the gap”
    - Example: If you cannot technically force passwords to have special characters, you can implement password policy
  - When a technical control, procedural control, or both are not available
COMMON ISSUES
Cannot amend existing TFE with new assets

EXAMPLE:

• You have existing TFE with 6 assets
• You want to add server to network
• You can’t add server to existing TFE
• You must create new TFE
  – Server will have new Safe Harbor date
Issues

• Evidence needs to be submitted timely
• Must explain how compensating measures provide equal or better protection than strict compliance
• Thoroughly explain mitigating measures/justification
  – NOT: “IT Dept. indicated we need a TFE”
• Provide sufficient evidence to support both justification and compensating measures
Provide robust evidence

• Example: Cannot add anti-virus to machine
• Not sufficient: Opinion document from an IT staffer
• We want to see:
  – Operating manual
  – Attestation from vendor company
  – Test results
Avoid Last-Minute Requests

- Appendix 4 D: *Submit TFE Request at least 60 calendar days before Compliant Date for Applicable Requirement*

- Last minute requests could push back CCA implementation or safe harbor date
Plan Ahead!

- Think about the need for TFEs while planning for CCAs
  - Not during or after implementing!
- Example: Entity installed Oracle DB server
  - Server had user account that could not conform to CIP-007 R 5.3
  - Led to numerous self-reported violations
Compensating measures must resolve vulnerabilities

- Ensure measures “close the gap”
  - Can’t solve logical vulnerability only with physical measures
  - Can’t solve physical vulnerability only with logical measures
Example: USB vulnerability

- **Does not solve:**
  - Firewall
  - Anti-virus
  - IDS/IPS

- **Appropriate measures:**
  - Physical controls
  - Disable port
  - Control who has access
Example: Unable to install Anti-Virus

• Appropriate measures:
  – Keep systems patched
  – Scan removable media on system that can run anti-virus before introducing to unprotected system

• Does not solve:
  – Physical access controls
Summary

- TFE needed for “safe harbor”
- Provide through justification and compensating/mitigating measures
- Be forward-thinking and plan ahead when changing and adding assets
  - Submit request at least 60 days before implementation
  - Start collecting evidence as soon as you know you need TFE