Comment Form

Project 2009-01 Disturbance and Sabotage Reporting

# 

Please DO NOT use this form for submitting comments. Please use the [electronic form](https://www.nerc.net/nercsurvey/Survey.aspx?s=b04b15af79ad48b6a6e9057f7cb157f0) to submit comments on the draft standard EOP-004-2. Comments must be submitted by May 24, 2012**.** If you have questions please contact [Stephen Crutchfield](mailto:stephen.crutchfield@nerc.net) by email or by telephone at (609) 651-9455.

### Background Information

# EOP-004-2 was posted for a 45-day formal comment period and initial ballot from October 28 through December 12, 2011. The DSR SDT received comments from stakeholders to improve the readability and clarity of the requirements of the standard. The revisions that were made to the standard are summarized in the following paragraphs.

# *Purpose Statement*

# The DSR SDT revised the purpose statement to remove ambiguous language “with the potential to impact reliability.” The Purpose statement now reads:

# “To improve the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.”

# *Operating Plan*

# Based on stakeholder comments, Requirement R1 was revised for clarity. Part 1.1 was revised to replace the word “identifying” with “recognizing” and Part 1.2 was eliminated. This also aligns the language of the standard with FERC Order 693, Paragraph 471.

# “(2) specify baseline requirements regarding what issues should be addressed in the procedures for recognizing {emphasis added} sabotage events and making personnel aware of such events;”

# Requirement R1, Part 1.3 (now Part 1.2) was revised by eliminating the phrase “as appropriate” and adding language indicating that the Responsible Entity is to define its process for reporting and with whom to report events. Part 1.2 now reads:

“1.2 A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity’s Reliability Coordinator; law enforcement, governmental or provincial agencies.”

# The SDT envisions that most entities will only need to slightly modify their existing CIP-001 Sabotage Reporting procedures to comply with the Operating Plan requirement in this proposed standard. As many of the features of both sabotage reporting procedures and the Operating Plan are substantially similar, the SDT feels that some information in the sabotage reporting procedures may need to updated and verified.

# *Operating Plan Review and Communications Testing*

# Requirement R1, Part 1.4 was removed and Requirement 1, Part, 1.5 was separated out as new Requirement 4. Requirement R4 was revised and is now R3. FERC Order 693, Paragraph 466 includes provisions for periodic review and update of the Operating Plan:

“466. The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures.”

# Requirement R3 requires an annual test of the communication portion of Requirement R1 while Requirement R4 requires an annual review of the Operating Plan.:

# “R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2.”

# “R4. Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1.”

# The DSR SDT envisions that the annual test will include verification that communication information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling “others as defined in the Responsibility Entity’s Operating Plan” (see Part 1.2) to verify that their contact information is up to date. If any discrepancies are noted, the Operating Plan would be updated. Note that there is no requirement to test the reporting of events to the Electric Reliability Organization and the Responsible Entity’s Reliability Coordinator.

# *Operating Plan Implementation*

# Most stakeholders indicated that Requirements R2 and R3 were redundant and having both in the standard was not necessary. Requirement R2 called for implementation of Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 called for reporting events in accordance with the Operating Plan. The DSR SDT deleted Requirement R2 based on stakeholder comments and revised R3 (now R2) to:

# “R2. Each Responsible Entity shall implement its event reporting Operating Plan for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment1.”

# *Reporting Timelines*

# The DSR SDT received many comments regarding the various entries of Attachment 1. Many commenters questioned the reliability benefit of reporting events to the ERO within 1 hour. Most of the events with a one hour reporting requirement were revised to 24 hours based on stakeholder comments; those types of events are currently required to be reported within 24 hours in the existing mandatory and enforceable standards. The only remaining type of event that is to be reported within one hour is “A reportable Cyber Security Incident” as it is required by CIP-008 and FERC Order 706, Paragraph 673:

# “direct the ERO to modify CIP-008 to require each responsible entity to contact appropriate government authorities and industry participants in the event of a cyber security incident as soon as possible, but in any event, within one hour of the event…”

# The table was reformatted to separate one-hour reporting and 24-hour reporting. The last column of the table was also deleted and the information contained in the table was transferred to the sentence above each table. These sentences are:

# “One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event.”

# “Twenty-four Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within twenty-four hour of recognition of the event.”

# Note that the reporting timeline of 24 hours starts when the situation has been determined as a threat, not when it may have first occurred.

# *Cyber-Related Events*

# The ‘Damage or Destruction’ events specifically relating to Critical Assets and Critical Cyber Assets were removed from Attachment 1. Stakeholders pointed out these events are adequately addressed through the CIP-008 and “Damage or Destruction of a Facility”reporting thresholds.

# CIP-008 addresses Cyber Security Incidents which are defined as:

# “Any malicious act or suspicious event that:

# • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a Critical Cyber Asset, or,

# • Disrupts, or was an attempt to disrupt, the operation of a Critical Cyber Asset.”

# A Critical Asset is defined as:

# “Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”

# Since there is an existing event category for damage or destruction of Facilities, having a separate event for “Damage or Destruction of a Critical Asset” is unnecessary.

# *Damage or Destruction*

# The event for “Destruction of BES equipment” has been revised to “Damage or destruction of a Facility”. The threshold for reporting information was expanded for clarity:

“Damage or destruction of a Facility that:

Affects an IROL (per FAC-014)

OR

Results in the need for actions to avoid an Adverse Reliability Impact

OR

# Results from actual or suspected intentional human action.”

# *Facility Definition*

# The DSR SDT used the defined term “Facility” to add clarity for this event as well as other events in Attachment 1. A Facility is defined as:

# “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)”

# The DSR SDT did not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

# *Physical Threats*

# Several stakeholders expressed concerns relating to the “Forced Intrusion” event. Their concerns related to ambiguous language in the footnote. The SDR SDT discussed this event as well as the event “Risk to BES equipment”. These two event types had perceived overlap in the reporting requirements. The DSR SDT removed “Forced Intrusion” as a category and the “Risk to BES equipment” event was revised to “Any physical threat that could impact the operability of a Facility”.

# Using judgment is unavoidable for this type of event. This language was chosen because the Responsible Entity is the best position to exercise this judgment and determine whether or not an event poses a threat to its Facilities. The DSR SDT believes this revised event type will minimize administrative burden and ensure that events meaningful to industry awareness are reported.

# The footnote regarding this event type was expanded to provide additional guidance in:

# “Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also, report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility.”

# *Use of DOE Form OE-417*

# The DSR SDT received many comments requesting consistency with DOE OE-417 thresholds and timelines. These items, as well as, the Events Analysis Working Group’s (EAWG) requirements were considered in creating Attachment 1, but differences remain for the following reasons:

# EOP-004 requirements were designed to meet NERC and the industry’s needs; accommodation of other reporting obligations was considered as an opportunity not a ‘must-have’

# OE-417 only applies to US entities, whereas EOP-004 requirements apply across North America

# NERC has no control over the criteria in OE-417, which can change at any time

# Reports made under EOP-004 provide a minimum set of information, which may trigger further information requests from EAWG as necessary

# In an effort to minimize administrative burden, US entities may use the OE-417 form rather than Attachment 2 to report under EOP-004. The SDT was informed by the DOE of its new online process coming later this year. In this process, entities may be able to record email addresses associated with their Operating Plan so that when the report is submitted to DOE, it will automatically be forwarded to the posted email addresses, thereby eliminating some administrative burden to forward the report to multiple organizations and agencies.

# *Miscellaneous*

# Other minor edits were made to Attachment 1. Several words were capitalized that are not defined terms. The DSR SDT did not intend for these terms to be capitalized (defined terms) and these words were reverted to lower case. The event type “Loss of monitoring or all voice communication capability” was divided into two separate events as “Loss of monitoring capability” and “Loss of all voice communication capability”.

# Attachment 2 was updated to reflect the revisions to Attachment 1. The reference to “actual or potential events” was removed. Also, the event type of “other” and “fuel supply emergency” was removed as well.

# It was noted that ‘Transmission Facilities’ is not a defined term in the NERC Glossary. Transmission and Facilities are separately defined terms. The combination of these two definitions are what the DSR SDT has based the applicability of “Transmission Facilities” in Attachment 1.

**You do not have to answer all questions.**

1. **The DSR SDT has revised EOP-004-2 by removing Requirement 1, Part 1.4 and separating Parts 1.3 and 1.5 into new Requirements R3 and R4. Requirement R3 calls for an annual test of the communications portion of the Operating Plan and Requirement R4 requires an annual review of the Operating Plan. Do you agree with this revision? If not, please explain in the comment area below.**

Yes

No

Comments:

1. **The DSR SDT made clarifying revisions to Attachment 1 based on stakeholder feedback. Do you agree with these revisions? If not, please explain in the comment area below.**

Yes

No

Comments:

1. **The DSR SDT has proposed a new Section 812 to be incorporated into the NERC Rules of Procedure. Do you agree with the proposed addition? If not, please explain in the comment area below.**

Yes

No

Comments:

1. **Do you have any other comment, not expressed in the questions above, for the DSR SDT?**

Comments: