Unofficial Comment Form

Disturbance and Sabotage Reporting (Project 2009-01)

Please **DO NOT** use this form to submit comments. Please use the [electronic comment form](https://www.nerc.net/nercsurvey/Survey.aspx?s=ec7c989da70c4737b7fb387d5af4ad27) to submit comments on the first formal posting for Project 2009-01—Disturbance and Sabotage Reporting. The electronic comment form must be completed by **December 12, 2011.**

[2009-01 Project Page](http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html)

If you have questions please contact Stephen Crutchfield at [stephen.crutchfield@nerc.net](mailto:stephen.crutchfield@nerc.net)

or by telephone at 609-651-9455.

**Background**

The DST SDT posted the draft standard EOP-004-2 for a formal comment period from March 9, 2011 through April 8, 2011. Based on stakeholder feedback, the DSR SDT made several revisions to the standard to improve clarity and address other concerns identified by stakeholders. The main stakeholder concerns were addressed as follows:

**Definition of Impact Event.** Many stakeholders disagreed with the need for the definition of “Impact Event” and felt that that the definition was ambiguous and created confusion. The DSR SDT agrees and has deleted the proposed definition from the standard. The list of events that are to be reported in Attachment 1 is inclusive and no further attempts to define ”Impact Event” are necessary.

**Timeframe for Reporting and Event.** Many stakeholders raised concerns with the one-hour reporting requirement for certain types of events. The commenters believed that the restoration of service or the return to a stable bulk power system state may be jeopardized by having to report certain events within one hour. The DSR SDT agreed and revised the reporting time to 24 hours for most events, with the exception of damage to or destruction of BES equipment, forced intrusion or cyber related incidents.

**VRFs.** Many stakeholders suggested that the reporting of events after the fact only justified a VRF of “lower” for each requirement. With the revised standard, there are now three requirements. Requirement 1 specifies that the responsible entity have an Operating Plan for identifying and reporting events listed in Attachment A. This is procedural in nature and justifies a “lower” VRF, as this requirement deals with the means to report events after the fact. The current approved VRFs for EOP-004-1 are all lower with the exception of Requirement R2 which is a requirement to analyze events. This standard relates only to reporting events. The analysis of reported events is addressed through the NERC Events Analysis Program in accordance with the NERC Rules of Procedure.

The three remaining requirements in EOP-004-2 require entities affected by events to report those events based on the specifics in Attachment A (Requirement R3) and to test the communications protocol of their Operating Plan once per year (R4). Requirement R2 provides for implementation of the Operating Plan as it relates to Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5. Requirement R3 specifies that an entity is responsible for reporting events to the appropriate entities in accordance with the Operating Plan based on Attachment A. Requirement R4 is intended to ensure that an entity can communicate information about events. Some of these events are potential sabotage events, and communicating these events is intended to make other entities aware to help prevent further sabotage events from occurring. Existing CIP-001-1a deals with sabotage events, and the approved VRFs for each of the requirements is “medium.” The proposed VRFs for EOP-004-2 are consistent with the existing approved VRFs for both EOP-004 and CIP-001.

**Applicability.** Commenters also had concerns about the applicability of the standard to Load Serving Entities, who may not own physical assets, as well as to the ERO and Regional Entity. The DSR SDT agrees that the Distribution Provider owns the assets per the Functional Model, however the LSE is an applicable entity under CIP-002, and under the CIP standards is responsible for reporting cyber security incidents. The ERO and RE are also responsible for reporting cyber security incidents under CIP-002. Therefore, the SDT determined that it was appropriate to include LSEs, the ERO and the RE in the applicability of EOP-004-2.

After the drafting team completed its consideration of stakeholder comments, the standards and implementation plan were submitted for quality review. Based on feedback from the quality review, the drafting team has made two significant revisions to the standard. The first revision is to add a requirement for implementation of the Operating Plan listed in Requirement R1. There was only a requirement to report events, but no requirement specifically calling for updates to the Operating Plan or the annual review. This was accomplished by having two requirements. The first is Requirement R2 which specifies that an entity must implement the Operating Plan per Requirement R1, Parts 1.1, 1.2, 1.4 and 1.5:

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

The second Requirement is R3 which addresses Part 1.3:

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

The second revision based on the quality review pertains to Requirement R4. The quality review suggested revising the requirement to more closely match the language in the Rationale box that the drafting team developed. This would provide better guidance for responsible entities as well as provide more clear direction to auditors. The revised requirement is:

R4. Each Responsible Entity shall verify (through actual implementation for an event, or through a drill or exercise) the communication process in its Operating Plan, created pursuant to Requirement 1, Part 1.3, at least annually (once per calendar year), with no more than 15 calendar months between verification or actual implementation.

**You do not have to answer all questions. Enter all comments in Simple Text Format.**

1. **The DSR SDT has revised EOP-004-2 to remove the training requirement R4 based on stakeholder comments from the second formal posting. Do you agree this revision? If not, please explain in the comment area below.**

Yes

No

Comments:

1. **The DSR SDT includes two requirement regarding implementation of the Operating Plan specified in Requirement R1. The previous version of the standard had a requirement to implement the Operating plan as well as a requirement to report events. The two requirements R2 and R3 were written to delineate implementation of the Parts of R1. Do you agree with these revisions? If not, please explain in the comment area below.**

R2. Each Responsible Entity shall implement the parts of its Operating Plan that meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts 1.4 and 1.5 as specified.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1.

Yes

No

Comments:

1. **The DSR SDT revised reporting times for many events listed in Attachment 1 from one hour to 24 hours. Do you agree with these revisions? If not, please explain in the comment area below.**

Yes

No

Comments:

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

Comments: