

## Unofficial Comment Form for Project 2009-01 — Disturbance and Sabotage Reporting

Please **DO NOT** use this form to submit comments. Please use the [form](#) located at the site below to submit comments on the proposed Concepts Paper for Disturbance and Sabotage Reporting. Comments must be submitted by **April 16, 2010**. If you have questions please contact Stephen Crutchfield by email at [.crutchfield@nerc.net](mailto:crutchfield@nerc.net) or by telephone at 609-651-9455.

[://www.nerc.com/filez/standards/Project2009-01\\_Disturbance\\_Sabotage\\_Reporting.html](http://www.nerc.com/filez/standards/Project2009-01_Disturbance_Sabotage_Reporting.html)

### **Background:**

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC Standards Committee in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009 and is progressing toward developing standards based on the SAR. The concepts paper was developed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed. Please review the redlined SAR and then answer the following questions.

This initial comment period is requesting industry input on the direction herein proposed by the DSR SDT. Should your organization feel that the direction proposed is not the direction that should be pursued then your comments on what direction the SDT should take would be greatly appreciated. The “concept paper” lays out the foundation for the reporting requirements in the standard. We are not seeking input or guidance on the definition of physical or cyber sabotage, what type of disturbances should be reported, who should do reporting, or to whom or what organizations will be receiving the reports. All of these points will be addressed by the SDT in later phases of the project and we will be seeking important industry guidance at those times. The SDT does recognize the importance of all of that data and information, but at this time, we are only seeking input on the direction of the concepts we propose to build upon.

1. The details of reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements. Do you agree with using the existing guidance as the foundation for disturbance reporting? Please explain your response (yes or no) in the comment area.

Yes

No

Comments: We agree with using the present documentation but would like just one reporting form. We are concerned that the guidelines and reporting periods specified within the DOE OE-417 report conflict with the NERC Guidelines. For example, DOE OE-417 report requires "Suspected Physical or Cyber Impairment" to be reported within 6 hours. The NERC guidelines indicate "Suspected Activities" are to be reported within 1 hour. We recommend the SDT use the DOE OE-417 report as a guiding document, and then determine additional reporting requirements using guidance from the NERC Guideline. FERC Order 693 appears to indicate conflicts and confusion with NERC reporting requirements and DOE reporting requirements should be eliminated.

2. The DSR SDT is considering developing a reporting hierarchy for disturbances that requires entities to submit information to the Reliability Coordinator and then for the Reliability Coordinator to submit the report. Do you agree with this hierarchy concept? Please explain your response (yes or no) in the comment area.

Yes

No

Comments: We agree a coordinated reporting process is beneficial for the entity and the Reliability Coordinator (RC). However, a hierarchy would likely lengthen the reporting timeframe, or reduce the allotted time for each entity to provide notification to the RC in order to meet DOE or NERC timelines. Communication and coordination with the RC would likely provide more accurate and complete data submissions within a timely process and create shared accountability for the report being submitted.

3. The goal of the DSR SDT is to have one report form for all functional entities (US, Canada, Mexico) to submit to NERC. Do you agree with this change? Please explain your response (yes or no) in the comment area.

Yes

No

Comments: However, We believe the primary goal should focus on "each entity" being able to submit one report for all functional requirements. Entities in the US that are required to submit the DOE OE-417 form should not be required to submit an additional form developed for other entities (Canada & Mexico). One approach to satisfy this goal is for NERC to require all entities (US, Canada, & Mexico) to complete the DOE OE-417 form as their report.

4. The goal of the DSR SDT is to eliminate the need to file duplicate reports. The standards will specify information required by NERC for reliability. To the extent that this information is also required for other reports (e.g. DOE OE-417), those reports will be allowed to supplement the NERC report in lieu of duplicating the entries in the NERC report. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Yes

No

Comments: We agree with the concept to eliminate duplicate reports. However, we are concerned with the reference of the DOE OE-417 report being a "supplement" of the NERC report rather than "accepted" as the NERC report.

5. In its discussion concerning sabotage, the DSR SDT has determined that the spectrum of all sabotage-type events is not well understood throughout the industry. In an effort to provide clarity and guidance, the DSR SDT developed the concept of an impact event. By developing impact events, it allows us to identify situations in the "gray area" where sabotage is not clearly defined. Other types of events may need to be reported for situational awareness and trend identification. Do you agree with this concept? Please explain your response (yes or no) in the comment area.

Yes

No

Comments: Rather than attempting to define a new term (impact event), we suggest that the concept of impact event be replaced with further defining sabotage and providing guidance on trigger events (impact event) that would cause an entity to report.

6. If you are aware of any regional reporting requirements beyond the scope of CIP-001, CIP-008 and EOP-004 please provide them here.

Comments: No comment.

7. If you have any other comments on the Concepts Paper that you haven't already provided in response to the previous questions, please provide them here.

Comments: Confusion often arises in the industry between the CIP standards and other reliability standards based on CIP-001 naming convention. We would suggest the SDT retire CIP-001 and incorporate requirements within the EOP-004 standard or a new EOP-xxx standard to avoid confusion rising from CIP and other NERC Reliability Standards.

Additionally, we assume the SDT has been created to specifically address FERC Order 693 directives to the ERO which appears to include the following items:

1. Applicability – "possible revisions to CIP-001-1 that address our concerns regarding the need for wider application of the Reliability Standard... the ERO should consider

whether separate, less burdensome requirements for smaller entities may be appropriate" (FERC, 2007, para. 460).

2. Definition of Sabotage – "we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event... we believe the term sabotage is commonly understood and that common understanding should suffice in most instances... the ERO should consider FirstEnergy's suggestions to differentiate between cyber and physical sabotage and develop a threshold of materiality." (FERC, 2007, para. 461-462)
3. Periodic Review and Testing – "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." (FERC, 2007, para. 466)
4. Redundant Reporting – "now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event... Regarding the potential for redundant reporting under CIP-001-1 and other government reporting standards, and the need for greater coordination... We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format... with the appropriate governmental agencies that have levied the reporting requirements." (FERC, 2007, para. 468-469)
5. Specified Time – "the Commission directs the ERO to modify CIP-001-1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specified period of time... the ERO should consider suggestions raised... to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage" (FERC, 2007, para. 470).
6. Summary of CIP-001-1 – "the Commission directs the ERO to develop the following modifications... (1) further define sabotage and provide guidance as to the triggering events... (2) specify baseline requirements regarding... procedures for recognizing sabotage events... (3) incorporate a periodic review... and for the periodic testing... (4) require an applicable specified period of time. In addition... address our concerns regarding applicability to smaller entities... consolidation of the sabotage reporting forms and the sabotage reporting channels with the appropriate governmental authorities to minimize the impact of these reporting requirements on all entities." (FERC, 2007, para. 471)
7. Analyze Performance – "at a minimum, generator operators and LSEs should analyze the performance of their equipment and provide the data... The Commission directs the ERO to consider this concern in future revisions... that includes any Requirements necessary for users, owners and operators... to provide data that will assist NERC" (FERC, 2007, para. 613, 617).

8. Reporting Time Frames – “The Commission directs the ERO to change its Rules of Procedures to assure that the Commission also receives these reports within the same time frames as the DOE.” (FERC, 2007, para. 618)