NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disturbance and Sabotage Reporting Standard Drafting Team (Project 2009-01) Reporting Concepts

Introduction

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. This concepts paper is designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The standards listed under the SAR are:

- CIP-001 — Sabotage Reporting
- EOP-004 — Disturbance Reporting

The DSR SDT is also proposing to investigate incorporation of the cyber incident reporting aspects of CIP-008 under this project. This will be coordinated with the Cyber Security — Order 706 Standard Drafting Team (Project 2008-06).

The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC database and FERC Order 693 Directives to determine a prudent course of action with respect to these standards.

This concept paper provides stakeholders with a proposed "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. This concept paper provides the background information and thought process of the DSR SDT.

The proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001 and EOP-004. The real-time reporting requirements are achieved through the RCIS and are covered in other standards (e.g. TOP). The proposed standards deal exclusively with after-the-fact reporting.

The DSR SDT is proposing to consolidate disturbance and event reporting under a single standard. These two components and other key concepts are discussed in the following sections.

Summary of Concepts and Assumptions:

The Standard Will: Require use of a single form to report disturbances and "impact events" that threaten the reliability of the bulk electric system

- Provide clear criteria for reporting
- Include consistent reporting timelines
- Identify appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provide clarity around of who will receive the information

The drafting team will explore other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements

Discussion of Disturbance Reporting

Disturbance reporting requirements currently exist in EOP-004. The current approved definition of Disturbance from the NERC Glossary of Terms is:

1. An unplanned event that produces an abnormal system condition.
2. Any perturbation to the electric system.
3. The unexpected change in ACE that is caused by the sudden failure of generation or interruption of load.

Disturbance reporting requirements and criteria are in the existing EOP-004 standard and its attachments. The DST 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, which will include clear criteria for reporting. The new/revised standard will specify who has access to reported information about disturbances.

The DSR SDT is considering developing a reporting hierarchy that requires the Reliability Coordinator (RC) to submit the disturbance report. Any entity (Distribution Provider, Load-Serving Entity, Generator Operator) that experiences a disturbance would report the appropriate information to the Transmission Operator or Balancing Authority (if applicable) who would then report to the RC. The RC would then submit the report to NERC, the affected Regional Entity (RE) and/or Department of Energy (DOE) as appropriate. By having the RC submit the report, situational awareness would be enhanced. All affected entities would be aware of the disturbance and relevant information. Also, the flow of information between entities would be enhanced and a more comprehensive report could be developed.

Discussion of "Impact Event" Reporting

There are situations worthy of reporting because they have the potential to impact reliability. The DSR SDT proposes calling such incidents 'impact events' with the following definition:

> An impact event is any situation that has the potential to significantly impact the reliability of the Bulk Electric System. Such events may originate from malicious intent, accidental behavior, or natural occurrences.

Impact event reporting facilitates situational awareness, which allows potentially impacted parties to prepare for and possibly mitigate the reliability risk. It also provides the raw material, in the case of certain potential reliability threats, to see emerging patterns.

Examples of impact events include:

- Bolts removed from transmission line structures
- Detection of cyber intrusion that meets criteria of CIP-008
- Forced intrusion attempt at a substation
- Train derailment near a transmission right-of-way
- Destruction of Bulk Electrical System equipment

What about sabotage?
One thing became clear in the DSR SDT's discussion concerning sabotage: everyone has a different definition. The current standard CIP-001 elicited the following response from FERC in FERC Order 693, paragraph 471 which states in part: *". . . the Commission directs the ERO to develop the following modifications to the Reliability Standard through the Reliability Standards development process: (1) further define sabotage and provide guidance as to the triggering events that would cause an entity to report a sabotage event."*

Often, the underlying reason for an event is unknown or cannot be confirmed. The DSR SDT believes that reporting material risks to the Bulk Electrical System using the impact event categorization, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

The DSR SDT discussed the reliability needs for impact event reporting and will consider guidance found in the document "NERC Guideline: Threat and Incident Reporting" in the development of requirements, which will include clear criteria for reporting.

Certain types of impact events should be reported to NERC, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and/or Provincial or local law enforcement. Other types of impact events may have different reporting requirements. For example, an impact event that is related to copper theft may only need to be reported to the local law enforcement authorities. The new standard will specify who has access to reported information about impact events.

Potential Uses of Reportable Information

Event analysis, correlation of data, and trend identification are a few potential uses for the information reported under this standard. As envisioned, the standard will only require Functional entities to report the incidents and provide information or data necessary for these analyses. Other entities (e.g. – NERC, Law Enforcement, etc) will be responsible for performing the analyses. The NERC Rules of Procedure (section 800) provide an overview of the responsibilities of the ERO in regards to analysis and dissemination of information for reliability.

Jurisdictional agencies (which may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE) have other duties and responsibilities.

Collection of Reportable Information or "One stop shopping"

The goal of the DSR SDT is to have one reporting form for all functional entities (US, Canada, Mexico) to submit to NERC. Ultimately, it may make sense to develop an electronic version to expedite completion, sharing and storage. Ideally, entities would complete a single form which could then be distributed to jurisdictional agencies and functional entities as appropriate. Specific reporting forms[1] that exist today (i.e. - OE-417, etc) could be included as part of the electronic form to accommodate US entities with a requirement to submit the form. Or may be removed (but still be mandatory for US entities under Public Law 93-275) to streamline the proposed consolidated reliability standard for all North American entities (US, Canada, Mexico). Jurisdictional agencies may include DHS, FBI, NERC, RE, FERC, Provincial Regulators, and DOE. Functional entities may include the RC, TOP, and BA for situational awareness. Applicability of the standard will be determined based on the specific requirements.

The DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT is planning to update the listing of reportable events from discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences may still exist.

The reporting proposed by the DSR SDT is intended to meet the uses and purposes of NERC. The DSR SDT recognizes that other requirements for reporting exist (e.g., DOE-417 reporting), which may duplicate or overlap the information required by NERC. To the extent that other reporting is required, the DSR SDT envisions that duplicate entry of information is not necessary, and the submission of the alternate report will be acceptable to NERC so long as all information required by NERC is submitted. For example, if the NERC Report duplicates information from the DOE form, the DOE report may be included or attached to the NERC report, in lieu of entering that information on the NERC report.

[1] The DOE Reporting Form, OE-417 is currently a part of the EOP-004 standard. If this report is removed from the standard, it should be noted that this form is still required by law as noted on the form: NOTICE: This report is mandatory under Public Law 93-275. Failure to comply may result in criminal fines, civil penalties and other sanctions as provided by law. For the sanctions and the provisions concerning the confidentiality of information submitted on this form, see General Information portion of the instructions. Title 18 USC 1001 makes it a criminal offense for any person knowingly and willingly to make to any Agency or Department of the United States any false, fictitious, or fraudulent statements as to any matter within its jurisdiction.