

Standard Development Timeline

This section is maintained by the drafting team during the development of the standard and will be removed when the standard becomes effective.

Development Steps Completed

1. SC approved SAR for initial posting (April, 2009).
2. SAR posted for comment (April 22 – May 21, 2009).
3. SC authorized moving the SAR forward to standard development (September 2009).
4. Concepts Paper posted for comment (March 17 – April 16, 2010).
5. Initial Informal Comment Period (September 2010)

Proposed Action Plan and Description of Current Draft

This is the first posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes, and proceed to second comment	October 2010 – February 2011
Second Comment Period	March – May 2011
Third Comment/Ballot period	June- July 2011
Recirculation Ballot period	July-August 2011
Receive BOT approval	September 2011

Effective Dates

1. The standard shall become effective on the first calendar day of the third calendar quarter after the date of the order providing applicable regulatory approval.
2. In those jurisdictions where no regulatory approval is required, the standard shall become effective on the first calendar day of the third calendar quarter after Board of Trustees adoption.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-1 Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-1a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting.	Revision to entire standard (Project 2009-01)

Definitions of Terms Used in Standard

This section includes all newly defined or revised terms used in the proposed standard. Terms already defined in the Reliability Standards Glossary of Terms are not repeated here. New or revised definitions listed below become approved when the proposed standard is approved. When the standard becomes effective, these defined terms will be removed from the individual standard and added to the Glossary.

Impact Event: Any event which has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.

When this standard has received ballot approval, the text boxes will be moved to the Guideline and Technical Basis Section.

Introduction

1. **Title:** Impact Event Reporting
2. **Number:** EOP-004-2
3. **Purpose:** To improve industry awareness and the reliability of the Bulk Electric System by requiring the reporting of Impact Events and their causes, if known, by the Responsible Entities.
4. **Applicability**
 - 4.1. **Functional Entities: Within the context of EOP-004-2, the term “Responsible Entity” shall mean:**
 - 4.1.1. Reliability Coordinator
 - 4.1.2. Balancing Authority
 - 4.1.3. Interchange Authority
 - 4.1.4. Transmission Service Provider
 - 4.1.5. Transmission Owner
 - 4.1.6. Transmission Operator
 - 4.1.7. Generator Owner
 - 4.1.8. Generator Operator
 - 4.1.9. Distribution Provider
 - 4.1.10 Load Serving Entity

5. Background:

NERC established a SAR Team in 2009 to investigate revisions to the CIP-001 and EOP-004 Reliability Standards.

1. CIP-001 may be merged with EOP-004 to eliminate redundancies.
2. Acts of sabotage have to be reported to the DOE as part of EOP-004.
3. Specific references to the DOE form need to be eliminated.
4. EOP-004 has some ‘fill-in-the-blank’ components to eliminate.

The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information).

The SAR for Project 2009-01, Disturbance and Sabotage Reporting was moved forward for standard drafting by the NERC SC in August of 2009. The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) was formed in late 2009. A “concepts paper” was designed to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT has developed.

The concept paper sought comments from stakeholders on the “road map” that will be used by the SDR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the SDR SDT.

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

The DSR SDT has used a working definition for “Impact Events” to develop Attachment 1 as follows:

“An Impact Event is any event that has either impacted or has the potential to impact the reliability of the Bulk Electric System. Such events may be caused by equipment failure or mis-operation, environmental conditions, or human action.”

The DSR SDT has proposed this definition for inclusion in the NERC Glossary for “Impact Event”. The types of Impact Events that are required to be reported are contained within Attachment 1. Only these events are required to be reported under this Standard. The DSR SDT considered the FERC directive to “further define sabotage” and decided to eliminate the term sabotage from the standard. The team felt that it was almost impossible to determine if an act or event was that of sabotage or merely vandalism without the intervention of law enforcement after the fact. This will result in further ambiguity with respect to reporting events. The term “sabotage” is no longer included in the standard and therefore it is inappropriate to attempt to define it. The Impact Events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive. Attachment 1, Part A is to be used for those actions that have impacted the electric system and in particular the section “Damage or destruction to equipment” clearly defines that all equipment that intentional or non intentional human error be reported. Attachment 1, Part B covers the similar items but the action has not fully occurred but may cause a risk to the electric system and is required to be reported.

To support this concept, the DSR SDT has provided specific event for reporting including types of Impact Events and timing thresholds pertaining to the different types of Impact Events and who’s responsibility for reporting under the different Impact Events. This information is outlined in Attachment 1 to the proposed standard.

The DSR SDT wishes to make clear that the proposed changes do not include any real-time operating notifications for the types of events covered by CIP-001, EOP-004. This is achieved

through the RCIS and is covered in other standards (e.g. TOP). The proposed standard deals exclusively with after-the-fact reporting.

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

Summary of Concepts

- A single form to report disturbances and Impact Events that threaten the reliability of the bulk electric system
- Other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Clear criteria for reporting
- Consistent reporting timelines
- Clarity around of who will receive the information and how it will be used

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting Impact Events. Certain outages, such as those due to vandalism and terrorism, are not preventable. Entities rely upon law enforcement agencies to respond and investigate those Impact Events which have the potential of wider area affect upon the industry which enables and supports reliability principles such as protection of bulk power systems from malicious physical or cyber attack. The Standard is intended to reduce the risk of Cascading involving Impact Events. The importance of BES awareness of the threat around them is essential to the effective operation and planning to mitigate the potential risk to the BES.

Stakeholders in the Reporting Process

- Industry
- NERC (ERO)
- FERC
- DOE
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State Law Enforcement
- FBI

The above stakeholders have an interest in the timely notification, communication and response to an incident at an industry facility. The stakeholders have various levels of accountability and have a vested interest in the protection and response to ensure the reliability of the BES.

Present expectations of the industry under CIP-001:

It has been the understanding by industry participants that an occurrence of sabotage has to be reported to the FBI. The FBI has the jurisdictional requirements to investigate acts of sabotage and terrorism. The present CIP-001-1 standard requires a liaison relationship on behalf of the industry and FBI. Annual requirements, under the standard, of the industry have not been clear and have lead to misunderstandings and confusion in the industry as to how to demonstrate the liaison is in place and effective. FBI offices have been asked to confirm, on FBI letterhead, the existence of a working relationship to report acts of sabotage to include references to years the liaison has been in existence and confirming telephone numbers for the FBI.

Coordination of Local and State Law Enforcement Agencies with the FBI

The Joint Terrorism Task Force (JTTF) came into being with the first task force being established in 1980. JTTFs are small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies. The JTTF is a multi-agency effort led by the Justice Department and FBI designed to combine the resources of federal, state, and local law enforcement. Coordination and communications largely through the interagency National Joint Terrorism Task Force, working out of FBI Headquarters, which makes sure that information and intelligence flows freely among the local JTTFs. This information flow can be most beneficial to the industry in analytical intelligence, incident response and investigation. Historically, the most immediate response to an industry incident has been local and state law enforcement agencies to suspected vandalism and criminal damages at industry facilities. Relying upon the JTTF coordination between local, state and FBI law enforcement would be beneficial to effective communications and the appropriate level of investigative response.

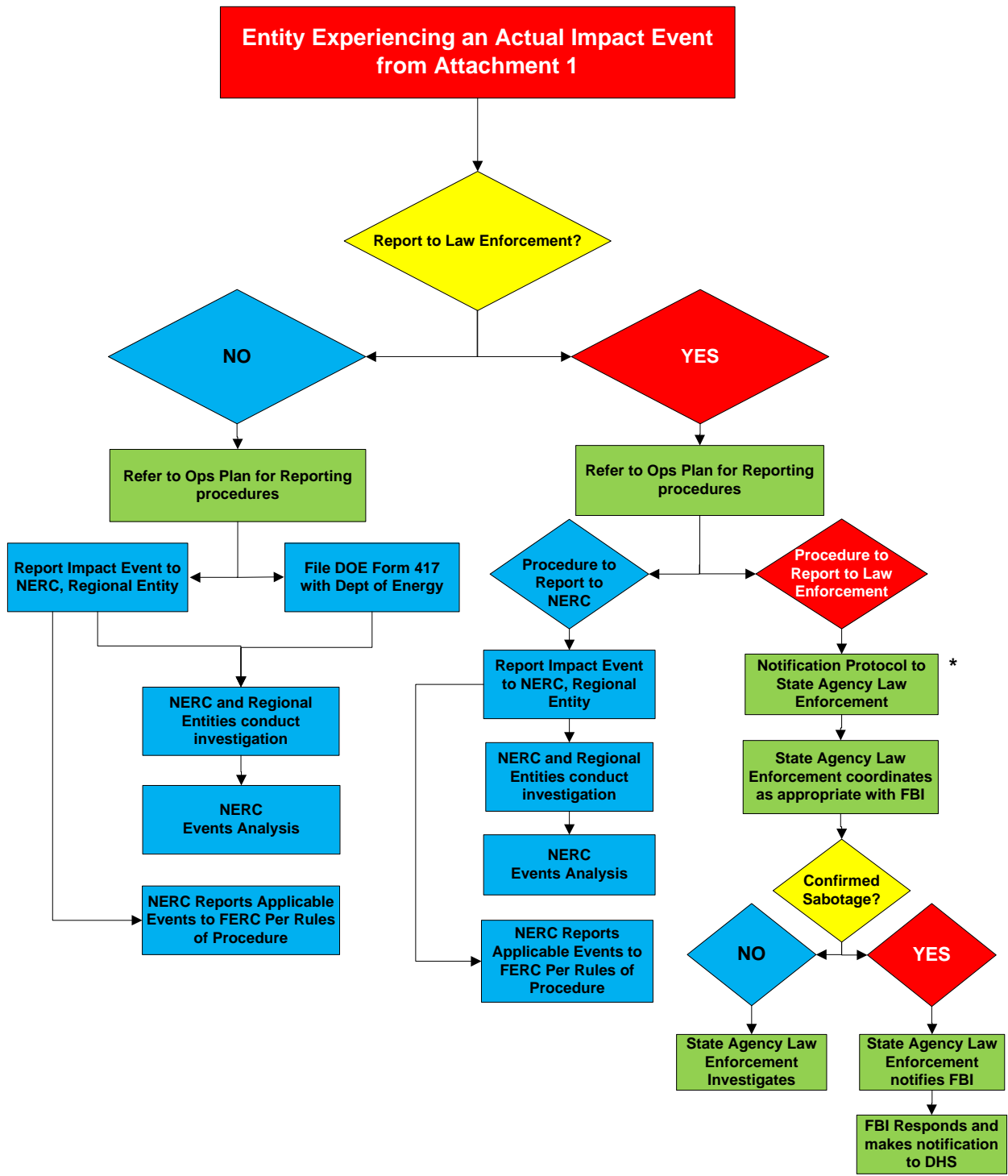
Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

A similar law enforcement coordination hierarchy exists in Canada. Local and Provincial law enforcement coordinate to investigate suspected acts of vandalism and sabotage. The Provincial law enforcement agency has a reporting relationship with the Royal Canadian Mounted Police (RCMP).

A Reporting Process Solution – EOP-004

A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Impact Event EOP-004-2). Essentially, reporting an Impact Event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierachy for Impact Event EOP-004-2



* Canadian entities will follow law enforcement protocols applicable in their jurisdictions

Requirements and Measures

R1. Each Responsible Entity shall have an Impact Event Operating Plan that includes: *[Violation Risk: Factor Medium] [Time Horizon: Long-term Planning]*

- 1.1. An Operating Process for identifying Impact Events listed in Attachment 1.
- 1.2. An Operating Procedure for gathering information for Attachment 2 regarding observed Impact Events listed in Attachment 1.
- 1.3. An Operating Process for communicating recognized Impact Events to the following:
 - 1.3.1. Internal company personnel notification(s).
 - 1.3.2. External organizations to notify to include but not limited to the Responsible Entities' Reliability Coordinator, NERC, Responsible Entities' Regional Entity, Law Enforcement, and Governmental or Provincial Agencies.
- 1.4. Provision(s) for updating the Impact Event Operating Plan within 90 days of any change to its content.

M1. Each Responsible Entity shall provide the current in force Impact Event Operating Plan to the Compliance Enforcement Authority.

R2. Each Responsible Entity shall implement its Impact Event Operating Plan documented in Requirement R1 for Impact Events listed in Attachment 1 (Parts A and B). *[Violation Risk: Factor Medium] [Time Horizon: Real-time Operations and Same-day Operations]*

M2. To the extent that an Responsible Entity has an Impact Event on its Facilities, the Responsible Entity shall provide documentation of the implementation of its Impact Event Operating Plans. Such evidence could include, but is not limited to, operator logs, voice

Rationale for R1

Every industry participant that owns or operates elements or devices on the grid has a formal or informal process, procedure, or steps it takes to gather information regarding what happened and why it happened when Impact Events occur. This requirement has the Registered Entity establish documentation on how that procedure, process, or plan is organized.

For the Impact Event Operating Plan, the DSR SDT envisions that Part 1.2 includes performing sufficient analysis and information gathering to be able to complete the report for reportable Impact Events. The main issue is to make sure an entity can a) identify when an Impact Event has occurred and b) be able to gather enough information to complete the report.

Part 1.3 could include a process flowchart, identification of internal positions to be notified and to make notifications, or a list of personnel by name as well as telephone numbers.

The Impact Event Operating Plan may include, but not be limited to, the following: how the entity is notified of event's occurrence, person(s) initially tasked with the overseeing the assessment or analytical study, investigatory steps typically taken, and documentation of the assessment / remedial action plan.

recordings, or other notations and documents retained by the Registered Entity for each Impact Event.

R3. Each Responsible Entity shall conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3 at least annually, with no more than 15 calendar months between tests.
[Violation Risk: Factor Medium]
[Time Horizon: Long-term Planning]

M3. In the absence of an actual Impact Event, the Responsible Entity shall provide evidence that it conducted a mock Impact Event and followed its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part 1.3. The time period between actual and or mock Impact Events shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or documentation. (R3)

Rationale for R3

The DSR SDT intends for each Responsible Entity to verify that its Operating Process for communicating recognized Impact Events is correct so that the entity can respond appropriately in the case of an actual Impact Event. The Responsible Entity may conduct a drill or exercise of its Operating Process for communicating recognized Impact Events as often as it desires but the time period between such drill or exercise can be no longer than 15 months from the previous drill/exercise or actual Impact Event (i.e., if you conducted an exercise/drill/actual employment of the Operating Process in January of one year, there would be another exercise/drill/actual employment by March 31 of the next calendar year)). Multiple exercises in a 15 month period are not a violation of the requirement and would be encouraged to improve reliability.

R4. Each Responsible Entity shall review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan at least annually with no more than 15 calendar months between review sessions*[Violation Risk: Factor Medium]* *[Time Horizon: Long-term Planning]*.

M4. Responsible Entities shall provide the materials presented to verify content and the association between the people listed in the plan and those who participated in the review, documentation showing who was present and when internal personnel were trained on the responsibilities in the plan.

R5. Each Responsible Entity shall report Impact Events in accordance with the Impact Event Operating Plan pursuant to Requirement R1 and Attachment 1 using the form in Attachment 2 or the DOE OE-417 reporting form. *[Violation Risk: Factor: Medium]*
[Time Horizon: Real-time Operations and Same-day Operations].

M5. Responsible Entities shall provide evidence demonstrating the submission of reports using the plan created pursuant to Requirement R1 and Attachment 1 using either the form in

Attachment 2 or the DOE OE-417 report. Such evidence will include a copy of the Attachment 2 form or OE-417 report submitted, evidence to support the type of Impact Event experienced; the date and time of the Impact Event; as well as evidence of report submittal that includes date and time.

Compliance

Compliance Enforcement Authority

- Regional Entity; or
- If the Responsible Entity works for the Regional Entity, then the Regional Entity will establish an agreement with the ERO or another entity approved by the ERO and FERC (i.e. another Regional Entity) to be responsible for compliance enforcement.

Compliance Monitoring and Enforcement Processes:

- Compliance Audits
- Self-Certifications
- Spot Checking
- Compliance Violation Investigations
- Self-Reporting
- Complaints

Evidence Retention

Each Responsible Entity shall retain data or evidence for three calendar years or for the duration of any regional or Compliance Enforcement Authority investigation; whichever is longer.

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until found compliant or for the duration specified above, whichever is longer.

The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

Additional Compliance Information

None

Table of Compliance Elements

R #	Time Horizon	VRF	Violation Severity Levels			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Long-term Planning	Medium	The Responsible Entity has an Impact Event Operating Plan but failed to include one of Parts 1.1 through 1.4.	The Responsible Entity has a Impact Event Operating Plan but failed to include two of Parts 1.1 through 1.4.	The Responsible Entity has an Impact Event Operating Plan but failed to include three of Parts 1.1 through 1.4.	The Responsible Entity failed to include all of Parts 1.1 through 1.4.
R2	Real-time Operations and Same-day Operations	Medium	N/A	N/A	N/A	The Responsible Entity failed to implement its Impact Event Operating Plan for an Impact Event listed in Attachment 1.
R3	Long-term Planning	Medium	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part	The Responsible Entity failed to conduct a test of its Operating Process for communicating recognized Impact Events created pursuant to Requirement R1, Part

EOP-004-2 — Impact Event Reporting

			1.3 in more than 15 months but less than 18 months.	1.3 in more than 18 months but less than 21 months.	1.3 in more than 21 months but less than 24 months.	1.3 in more than 24 months
R4	Long-term Planning	Medium	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 15 months but less than 18 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 18 months but less than 21 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 21 months but less than 24 months.	The Responsible Entity failed to review its Impact Event Operating Plan with those personnel who have responsibilities identified in that plan in more than 24 months
R5	Real-time Operations and Same-day Operations	Medium	The Responsible Entity failed to submit a report in less than 36 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 36 hours but less than or equal to 48 hours for an Impact Event requiring reporting within 24 hours in Attachment 1.	The Responsible Entity failed to submit a report in more than 48 hours but less than or equal to 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 1 hour but less than 2 hours for an Impact Event requiring reporting within 1 hour in Attachment 1.	The Responsible Entity failed to submit a report in more than 60 hours for an Impact Event requiring reporting within 24 hours in Attachment 1. OR The Responsible Entity failed to submit a report in more than 2 hours for an Impact Event requiring reporting within 1 hour in Attachment 1. OR The responsible entity failed to submit a

EOP-004-2 — Impact Event Reporting

						report for an Impact Event in Attachment 1.
--	--	--	--	--	--	---

Variations

None

Interpretations

None

EOP-004 - Attachment 1: Impact Events Table

NOTE: Under certain adverse conditions, e.g. severe weather, it may not be possible to report the damage caused by an Impact Event and issue a written Impact Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify its Regional Entity(ies) and NERC, (e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422) and provide as much information as is available. The affected Responsible Entity shall then provide periodic verbal updates until adequate information is available to issue a written Impact Event report.

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	Entity with Reporting Responsibility	Threshold for Reporting	Time to Submit Report
Energy Emergency requiring Public appeal for load reduction	Initiating entity is responsible for reporting	Each public appeal for load reduction	Within 1 hour of issuing a public appeal
Energy Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more	Within 1 hour after event is initiated
Energy Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW	Within 1 hour after event is initiated
Energy Emergency resulting in automatic firm load shedding	Each DP or TOP that experiences the Impact Event	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	Within 1 hour after event is initiated
Voltage Deviations on BES Facilities	Each RC, TOP, GOP that experiences the Impact Event	$\pm 10\%$ sustained for ≥ 15 continuous minutes	Within 24 hours after 15 minute threshold
IROL Violation	Each RC, TOP that experiences the Impact Event	Operate outside the IROL for time greater than IROL T_v	Within 24 hours after T_v threshold
Loss of Firm load for ≥ 15 Minutes	Each RC, BA, TOP, DP that experiences the Impact Event	<ul style="list-style-type: none"> • ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities 	Within 1 hour after 15 minute threshold
System Separation	Each RC, BA, TOP, DP that	Each separation resulting in an island of	Within 1 hour after occurrence is

EOP-004-2 — Impact Event Reporting

EOP-004 – Attachment 1 - Actual Reliability Impact – Part A			
Event	Entity with Reporting Responsibility	Threshold for Reporting	Time to Submit Report
(Islanding)	experiences the Impact Event	generation and load \geq 100 MW	identified
Generation loss	Each RC, BA, GOP that experiences the Impact Event	<ul style="list-style-type: none"> \geq 2,000 MW for entities in the Eastern or Western Interconnection \geq 1000 MW for entities in the ERCOT or Quebec Interconnection 	Within 24 hours after occurrence
Loss of Off-site power to a nuclear generating plant (grid supply)	Each RC, BA, TO, TOP, GO, GOP that experiences the Impact Event	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement	Report within 24 hours after occurrence
Transmission loss	Each RC, TOP that experiences the Impact Event	Three or more BES Transmission Elements	Within 24 hours after occurrence
Damage or destruction of BES equipment ¹	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the Impact Event	Through operational error, equipment failure, external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified
Damage or destruction of Critical Asset	Applicable Entities under CIP-002 or its successor.	Through operational error, equipment failure, external cause, or intentional or unintentional human action.	Within 1 hour after occurrence is identified
Damage or destruction of a Critical Cyber Asset	Applicable Entities under CIP-002 or its successor.	Through intentional or unintentional human action.	Within 1 hour after occurrence is identified

¹BES equipment that: i) Affects an IROL; ii) Significantly affects the reliability margin of the system (e.g., has the potential to result in the need for emergency actions); iii) Damaged or destroyed due to intentional or unintentional human action; or iv) Do not report copper theft from BES equipment unless it degrades the ability of equipment to operate correctly e.g., removal of grounding straps rendering protective relaying inoperative.

EOP-004-2 — Impact Event Reporting

EOP-004 – Attachment 1 - Potential Reliability Impact – Part B			
Event	Entity with Reporting Responsibility	Threshold for Reporting	Time to Submit Report
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential Impact Event	Unplanned evacuation from BES control center facility	Report within 24 hour after occurrence
Fuel supply emergency	Each RC, BA, GO, GOP that experiences the potential Impact Event	Affecting BES reliability ²	Report within 1 hour after occurrence
Loss of all monitoring or voice communication capability	Each RC, BA, TOP that experiences the potential Impact Event	Affecting a BES control center for ≥ 30 continuous minutes	Report within 24 hours after occurrence
Forced intrusion ³	Each RC, BA, TO, TOP, GO, GOP that experiences the potential Impact Event	At a BES facility	Report within 1 hour after verification of intrusion

² Report if problems with the fuel supply chain result in the projected need for emergency actions to manage reliability.

³ Report if you cannot reasonably determine likely motivation (i.e., intrusion to steal copper or spray graffiti is not reportable unless it effects the reliability of the BES).

EOP-004-2 — Impact Event Reporting

Risk to BES equipment ⁴	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	From a non-environmental physical threat	Report within 1 hour after identification
Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the potential Impact Event	That meets the criteria in CIP-008 (or its successor)	Report within 1 hour after detection

⁴ Examples include a train derailment adjacent to BES equipment, that either could have damaged the equipment directly or has the potential to damage the equipment (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a BES facility control center) and report of suspicious device near BES equipment).

EOP-004-2 — Impact Event Reporting

EOP-004 - Attachment 2: Impact Event Reporting Form

This form is to be used to report Impact Events to the ERO. NERC will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Reports should be submitted via one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550

Impact Event Reporting for EOP-004-2		
	Task	Comments
1.	Entity filing the report (include company name and Compliance Registration ID number):	
2.	Date and Time of Impact Event. Date: (mm/dd/yyyy) Time/Zone:	
3.	Name of contact person: Email address: Telephone Number:	
4.	Did the actual or potential Impact Event originate in your system?	Actual Impact Event <input type="checkbox"/> Potential Impact Event <input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown <input type="checkbox"/>
5.	Under which NERC function are you reporting? (RC, TOP, BA, other)	

EOP-004-2 — Impact Event Reporting

Impact Event Reporting for EOP-004-2			
	Task	Comments	
6.	Brief Description of actual or potential Impact Event: (More detail should be provided in the Sequence of Events section below.)		
7.	Generation tripped off-line*. MW Total List units tripped		
8.	Frequency*. Just prior to Impact Event (Hz): Immediately after Impact Event (Hz max): Immediately after Impact Event (Hz min):		
9.	List transmission facilities (lines, transformers, buses, etc.) tripped and locked-out*. (Specify voltage level of each facility listed).		
10.	Demand tripped (MW)*: Number of affected customers*:	FIRM	INTERRUPTIBLE

Impact Event Reporting for EOP-004-2			
	Task	Comments	
	Demand lost (MW-Minutes)*:		
11.	Restoration Time*.	INITIAL	FINAL
	Transmission:		
	Generation:		
	Demand:		
12.	Sequence of Events of actual or potential Impact Event (if potential Impact Event, please describe your assessment of potential impact to BES) :		

Impact Event Reporting for EOP-004-2	
Task	Comments
13.	Identify the initial probable cause or known root cause of the actual or potential Impact Event if known at time of submittal of Part I of this report:
14.	Identify any protection system misoperation(s) ¹ :
15.	Additional Information that helps to further explain the actual or potential Impact Event if needed.

¹ Only applicable if it is part of the impact event the responsible entity is reporting on

Guideline and Technical Basis

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 also proposed 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 SDT (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. EOP-002-Capacity and Energy Emergencies). 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 DSR SDT discussed the reliability needs for disturbance reporting and developed the list of Impact Events that are to be reported under this standard (attachment 1).

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 concept:

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 industry 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 or its successor standard
- 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 DST 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.

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 forms⁶ that exist today (i.e. - OE-417, etc) could be included as part of the

⁶ 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

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 industry 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.

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.