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 15 – October 15, 2010)
6. Second Comment Period (Formal) (March 9 – April 8, 2011)

Proposed Action Plan and Description of Current Draft
This is the third posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 45-day formal comment period concurrent with the formation of the ballot pool and the initial ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on second posting	April - October 2011
Third Comment/Ballot period	November-December 2011
Recirculation Ballot period	December 2011
Receive BOT approval	February 2012

Effective Dates

EOP-004-2 shall become effective on the first day of the third calendar quarter after applicable regulatory approval. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the third calendar quarter after Board of Trustees approval.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Impact Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-4, Requirement 1, Part 1.3.	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.

None

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

A. Introduction

1. Title: 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 events with the potential to impact reliability 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 Coordinator

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

4.1.11. Electric Reliability Organization

4.1.12. Regional Entity

5. Background:

NERC established a SAR Team in 2009 to investigate and propose revisions to the CIP-001 and EOP-004 Reliability Standards. The team was asked to consider the following:

1. CIP-001 could 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 had some 'fill-in-the-blank' components to eliminate.

The development included 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.

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.

The DSR SDT developed a concept paper to solicit stakeholder input regarding the proposed reporting concepts that the DSR SDT had developed. The posting of the concept paper sought comments from stakeholders on the "road map" that will be used by the DSR SDT in updating or revising CIP-001 and EOP-004. The concept paper provided stakeholders the background information and thought process of the DSR SDT. The DSR SDT has reviewed the existing standards, the SAR, issues from the NERC issues database and FERC Order 693 Directives in order to determine a prudent course of action with respect to revision of these standards.

Summary of Key Concepts

The DSRSDT identified the following principles to assist them in developing the standard:

- Develop a single form to report disturbances and events that threaten the reliability of the bulk electric system
- Investigate other opportunities for efficiency, such as development of an electronic form and possible inclusion of regional reporting requirements
- Establish clear criteria for reporting
- Establish consistent reporting timelines
- Provide clarity around who will receive the information and how it will be used

During the development of concepts, the DSR SDT considered the FERC directive to "further define sabotage". There was concern among stakeholders that a definition may be ambiguous and subject to interpretation. Consequently, the DSR SDT 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 sabotage or vandalism without the intervention of law enforcement. The DSR SDT felt that attempting to define sabotage would result in further ambiguity with respect to reporting events. The term "sabotage" is no longer included in the standard. The events listed in Attachment 1 were developed to 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.

The types of events that are required to be reported are contained within Attachment 1. The DSR SDT has coordinated with the NERC Events Analysis Working Group to develop the list of events that are to be reported under this standard. Attachment 1, Part A pertains to those actions or events that have impacted the Bulk Electric System. These events were previously reported under EOP-004-1, CIP-001-1 or the Department of Energy form OE-417. Attachment 1, Part B covers similar items that may have had an impact on the Bulk Electric System or has the potential to have an impact and should be reported.

The DSR SDT wishes to make clear that the proposed Standard does not include any real-time operating notifications for the events listed in Attachment 1. Real-time reporting is achieved through the RCIS and is covered in other standards (e.g. the TOP family of standards). The proposed standard deals exclusively with after-the-fact reporting.

Data Gathering

The requirements of EOP-004-1 require that entities "promptly analyze Bulk Electric System disturbances on its system or facilities" (Requirement R2). The requirements of EOP-004-2 specify that certain types of events are to be reported but do not include provisions to analyze events. Events reported under EOP-004-2 may trigger further scrutiny by the ERO Events Analysis Program. If warranted, the Events Analysis Program personnel may request that more data for certain events be provided by the reporting entity or other entities that may have experienced the event. Entities are encouraged to become familiar with the Events Analysis Program and the NERC Rules of Procedure to learn more about with the expectations of the program.

Law Enforcement Reporting

The reliability objective of EOP-004-2 is to prevent outages which could lead to Cascading by effectively reporting events. Certain outages, such as those due to vandalism and terrorism, may not be reasonably preventable. These are the types of events that should be reported to law enforcement. Entities rely upon law enforcement agencies to respond to and investigate those events which have the potential to impact a wider area of the BES. The inclusion of reporting to law enforcement 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 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), Regional Entity
- FERC
- DOE
- NRC
- DHS – Federal
- Homeland Security- State
- State Regulators
- Local Law Enforcement
- State or Provincial Law Enforcement
- FBI
- Royal Canadian Mounted Police (RCMP)

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-001-1a:

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 CIP-001-1-1a standard requires a liaison relationship on behalf of the industry and the FBI or RCMP. 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 that the liaison is in place and effective. As an example of proof of compliance with Requirement R4, responsible entities have asked FBI Office personnel to provide, on FBI letterhead, confirmation of the existence of a working relationship to report acts of sabotage, , the number of years the liaison relationship has been in existence, and the validity of the 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, 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.

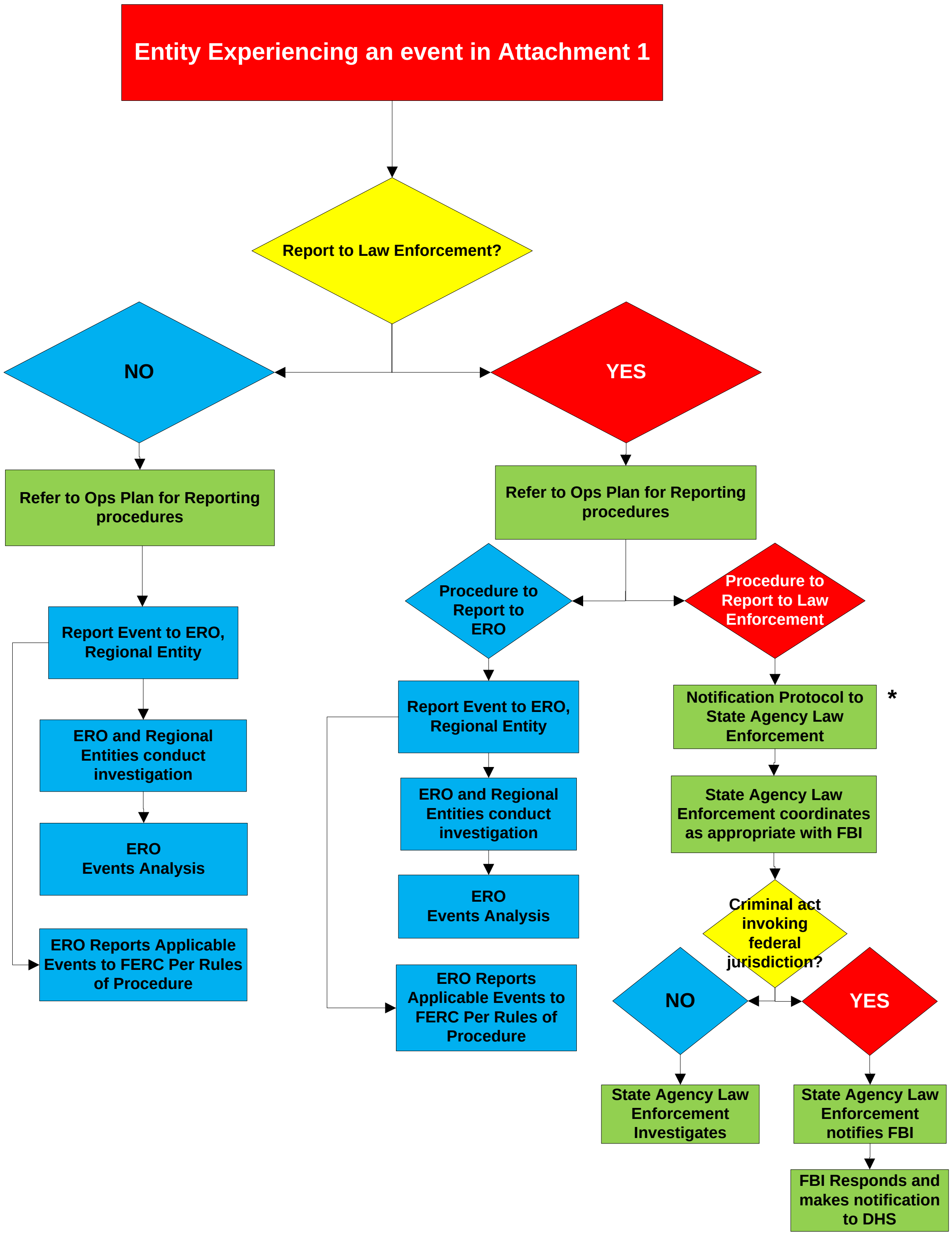
Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

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 the FBI, FERC Staff, NERC Standards Project Coordinator and the SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Reportable Events). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial or local level law enforcement agency. The state or provincial or local level law enforcement agency will coordinate with law enforcement with jurisdiction to investigate. If the state or provincial or local level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial or local level law enforcement agency will notify and coordinate with the FBI or the RCMP.

Reporting Hierarchy for Reportable Events



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

B. Requirements and Measures

R1. Each Responsible Entity shall have an Operating Plan that includes: *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

1.1. A process for identifying events listed in Attachment 1.

1.2. A process for gathering information for Attachment 2 regarding events listed in Attachment 1.

1.3. A process for communicating events listed in Attachment 1 to the Electric Reliability Organization, the Responsible Entity's Reliability Coordinator and the following as appropriate:

- Internal company personnel
- The Responsible Entity's Regional Entity
- Law enforcement
- Governmental or provincial agencies

1.4. Provision(s) for updating the Operating Plan within 90 calendar days of any change in assets, personnel, other circumstances that may no longer align with the Operating Plan; or incorporating lessons learned pursuant to Requirement R3.

1.5. A Process for ensuring the responsible entity reviews the Operating Plan at least annually (once each calendar year) with no more than 15 months between reviews.

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 when events occur. This requirement has the Responsible Entity establish documentation on how that procedure, process, or plan is organized. This documentation may be a single document or a combination of various documents that achieve the reliability objective.

For the Operating Plan, Part 1.2 includes information gathering to be able to complete the report for reportable events. The main issue is to make sure an entity can a) identify when an 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 and external personnel or entities to be notified, or a list of personnel by name and their associated telephone numbers.

M1. Each Responsible Entity will provide the current, dated, in force Operating Plan which includes Parts 1.1 - 1.5 as requested.

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*.

M2. Responsible Entities shall provide evidence that it implemented the parts of its Operating Plan to meet Requirement R1, Parts 1.1 and 1.2 for an actual event and Parts, 1.4 and 1.5 as specified. Evidence may include, but is not limited to, an event report form (Attachment 2) or the OE-417 report submitted, operator logs, voice recordings, or dated documentation of review and update of the Operating Plan. (R2)

Rationale for R2

Each Responsible Entity must implement the various parts of Requirement R1. Parts 1.1 and 1.2 call for identifying and gathering information for actual events. Parts 1.4 and 1.5 require updating and reviewing the Operating Plan.

R3. Each Responsible Entity shall report events in accordance with its Operating Plan developed to address the events listed in Attachment 1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*.

M3. Responsible Entities shall provide a record of the type of event experienced; a dated copy of the Attachment 2 form or OE-417 report; and dated and time-stamped transmittal records to show that the event was reported. (R3)

Rationale for R3

Each Responsible Entity must report events via its Operating Plan based on Attachment 1. For each event listed in Attachment 1, there are entities listed that are to be notified as well as the time required to perform the reporting.

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. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Rationale for R4

Each Responsible Entity must verify that its Operating Plan for communicating events is correct so that the entity can respond appropriately in the case of an actual event. The Responsible Entity may conduct a drill or exercise to test its Operating Plan for communicating events as often as it desires but the time period between tests can be no longer than 15 calendar months from the previous drill/exercise or actual event (i.e., if you conducted an exercise/drill/actual employment of the Operating Plan 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.

Evidence showing that an entity used the communication process in its Operating Plan for an actual event qualifies as evidence to meet this requirement.

M4. The Responsible Entity shall provide evidence that it verified the communication process in its Operating Plan for events created pursuant to Requirement R1, Part 1.3. Either implementation of the communication process as documented in its Operating Plan for an actual event or documented evidence of a drill or exercise may be used as evidence to meet this requirement. The time period between an actual event or verification shall be no more than 15 months. Evidence may include, but is not limited to, operator logs, voice recordings, or dated documentation of a verification. (R3)

C. Compliance

1. Compliance Monitoring Process

1.1 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; or

Third-party monitor without vested interest in the outcome for the ERO

.

1.2 Evidence Retention

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the Compliance Enforcement Authority may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

Each Responsible Entity shall retain the current, in force document plus the 'dated revision history' from each version issued since the last audit for 3 calendar years for Requirement R1 and Measure M1.

Each Responsible Entity shall retain evidence from prior 3 calendar years for Requirements R2, R3, R4, and Measures M2, M3, M4.

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.

1.3 Compliance Monitoring and Enforcement Processes:

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

1.4 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	Lower	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include one of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include two of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity has an Operating Plan but failed to include three of Parts 1.1 through 1.5.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to include four or more of Parts 1.1 through 1.5.
R2	Real-time Operations and Same-day Operations	Medium	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: N/A 1.2: N/A 1.4: The Reliability Coordinator, Balancing Authority,	1.1: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 90 days of a change, but not more than 100 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more	Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 100 days of a change, but not more than 110 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 18 calendar	Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 110 days of a change, but not more than 120 days after a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 21 calendar	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for identifying events. 1.2: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to implement the process for gathering information for Attachment 2. 1.4: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			than 15 calendar months after its previous review, but not more than 18 calendar months after its previous review.	months after its previous review, but not more than 21 calendar months after its previous review.	months after its previous review, but not more than 24 calendar months after its previous review.	Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to update the Operating Plan more than 120 days of a change. 1.5: The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity reviewed the Operating Plan, more than 24 calendar months after its previous review.
R3	Real-time Operations and Same-day Operations	Medium	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator

			Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 24 hours but less than or equal to 36 hours after an event requiring reporting within 24 hours in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 36 hours but less than or equal to 48 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 48 hours but less than or equal to 60 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in Attachment 1.	Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 60 hours after an event requiring reporting within 24 hours in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in Attachment 1. OR The Reliability Coordinator, Balancing Authority, Interchange Coordinator,

						Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to submit a report for an event in Attachment 1.
R4	Operations Planning	Medium	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 15 calendar months after its previous test, but not more than 18 calendar months after its previous test. OR	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 18 calendar months after its previous test, but not more than 21 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 21 calendar months after its previous test, but not more than 24 months after its previous test.	The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity verified the communication process in its Operating Plan, more than 24 calendar months after its previous test. OR The Reliability Coordinator, Balancing Authority, Interchange

			The Reliability Coordinator, Balancing Authority, Interchange Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan within the calendar year.			Coordinator, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Distribution Provider or Load Serving Entity failed to verify the communication process in its Operating Plan.

D. Variances

None.

E. Interpretations

None.

F. Interpretations

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Events Table

NOTE: Under certain adverse conditions (e.g. severe weather, multiple events) it may not be possible to report the damage caused by an event and issue a written Event Report within the timing in the table below. In such cases, the affected Responsible Entity shall notify parties per R1 and provide as much information as is available at the time of the notification. The affected Responsible Entity shall provide periodic verbal updates until adequate information is available to issue a written Event report. Reports to the ERO should be submitted to one of the following: e-mail: esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422.

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
Destruction of BES equipment[1]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the destruction of BES equipment	Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Damage or destruction of Critical Asset per CIP-002	Applicable Entities under CIP-002	Initial indication the event was due to operational error, equipment failure, external cause, or intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Damage or destruction of a Critical Cyber Asset per CIP-002	Applicable Entities under CIP-002.	Through intentional or unintentional human action.	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Forced intrusion[2]	Each RC, BA, TO, TOP, GO, GOP that experiences the	At a BES facility	The parties identified pursuant to R1.3 within 1 hour of recognition of

[1]BES 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 which removes the BES equipment from service. 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).

[2] 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).

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
	forced intrusion		event.
Risk to BES equipment[3]	Each RC, BA, TO, TOP, GO, GOP, DP that experiences the risk to BES equipment	From a non-environmental physical threat	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
Detection of a reportable Cyber Security Incident.	Each RC, BA, TO, TOP, GO, GOP, DP, ERO or RE that experiences the Cyber Security Incident	That meets the criteria in CIP-008	The parties identified pursuant to R1.3 within 1 hour of recognition of event.
BES Emergency requiring public appeal for load reduction	Deficient entity is responsible for reporting	Each public appeal for load reduction	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more	The parties identified pursuant to R.1.3 within 24 hours of recognition of the event.
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
BES Emergency resulting in automatic firm load shedding	Each DP or TOP that experiences the automatic load shedding	Firm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)	The parties identified pursuant to R1.3 within 24 hours of recognition of the event.
Voltage deviations on BES Facilities	Each TOP that experiences the voltage deviation	± 10% sustained for ≥ 15 continuous minutes	The parties identified pursuant to R1.3 within 24 hours after 15 minutes of exceeding the threshold.

[3] 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.

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
IROL Violation (all Interconnections) or SOL Violation (WECC only)	Each RC that experiences the IROL Violation (all Interconnections) or SOL violation (WECC only)	Operate outside the IROL for time greater than IROL Tv (all Interconnections) or Operate outside the SOL for a time greater than the SOL Tv (WECC only).	The parties identified pursuant to R1.3 within 24 hours after exceeding the Tv threshold.
Loss of Firm load for ≥ 15 Minutes	Each BA, TOP, DP that experiences the loss of firm load	• ≥ 300 MW for entities with previous year's demand ≥ 3000 MW • ≥ 200 MW for all other entities	The parties identified pursuant to R1.3 24 hours after exceeding the 15 minute threshold
System Separation (Islanding)	Each RC, BA, TOP, DP that experiences the system separation	Each separation resulting in an island of generation and load ≥ 100 MW	The parties identified pursuant to R1.3 within 24 hours after occurrence is identified
Generation loss	Each BA, GOP that experiences the generation loss	• ≥ 2,000 MW for entities in the Eastern or Western Interconnection • ≥ 1000 MW for entities in the ERCOT or Quebec Interconnection	The parties identified pursuant to R1.3within 24 hours after occurrence.
Loss of Off-site power to a nuclear generating plant (grid supply)	Each TO, TOP that experiences the loss of off-site power to a nuclear generating plant	Affecting a nuclear generating station per the Nuclear Plant Interface Requirement	The parties identified pursuant to R1.3 within 24 hours after occurrence
Transmission loss	Each TOP that experiences the transmission loss	Unintentional loss of Three or more Transmission Facilities (excluding successful automatic reclosing)	The parties identified pursuant to R1.3 within 24 hours after occurrence
Unplanned Control Center evacuation	Each RC, BA, TOP that experiences the potential event	Unplanned evacuation from BES control center facility	The parties identified pursuant to R1.3 within 24 hours of recognition of event.
Loss of monitoring or all voice	Each RC, BA, TOP that experiences the loss of	Voice Communications: Affecting a BES control center for ≥ 30 continuous minutes	The parties identified pursuant to R1.3 within 24 hours of recognition

Attachment 1 - Reportable Events			
Event	**Entity with Reporting Responsibility**	**Threshold for Reporting**	**Submit Attachment 2 or DOE OE-417 Report to:**
communication capability	monitoring or all voice communication capability	Monitoring: Affecting a BES control center for ≥ 30 continuous minutes such that analysis tools (State Estimator, Contingency Analysis) are rendered inoperable.	of event.

EOP-004 - Attachment 2: Event Reporting Form

<table>
<tr><td colspan="3">EOP-004, Attachment 2: Event Reporting Form
This form is to be used to report events to parties listed in Attachment 1, column labeled “Submit Attachment 2 or DOE OE-417 Report to:”. These parties 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, voice: 609-452-1422.</td></tr>
<tr><th colspan="2">Task</th><th>Comments</th></tr>
<tr><td>1.</td><td>Entity filing the report include:
Company name:
Name of contact person:
Email address of contact person:
Telephone Number:
Submitted by (name):</td><td></td></tr>
<tr><td>2.</td><td>Date and Time of recognized event.
Date: (mm/dd/yyyy)
Time: (hh:mm)
Time/Zone:</td><td></td></tr>
<tr><td>3.</td><td>Did the actual or potential event originate in your system?</td><td>Actual event ☐ Potential event ☐
Yes ☐ No☐ Unknown ☐</td></tr>
<tr><td rowspan="2">4.</td><td colspan="2">Event Identification and Description:</td></tr>
<tr><td>(Check applicable box)
☐ public appeal
☐ voltage reduction
☐ manual firm load shedding
☐ firm load shedding(undervoltage, underfrequency, SPS/RAS)
☐ voltage deviation
☐ IROL violation</td><td>Written description (optional unless Other is checked):</td></tr>
</table>

EOP-004, Attachment 2: Event Reporting Form		
This form is to be used to report events to parties listed in Attachment 1, column labeled "Submit Attachment 2 or DOE OE-417 Report to:". These parties 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, voice: 609-452-1422.		
	Task	**Comments**
	☐ loss of firm load ☐ system separation(islanding) ☐ generation loss ☐ loss of off-site power to nuclear generating plant ☐ transmission loss ☐ damage or destruction of BES equipment ☐ damage or destruction of Critical Asset ☐ damage or destruction of Critical Cyber Asset ☐ unplanned control center evacuation ☐ fuel supply emergency ☐ loss of all monitoring or voice communication capability ☐ forced intrusion Risk to BES equipment ☐ reportable Cyber Security Incident ☐ other	

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 has developed updated standards based on the SAR.

The standards listed under the SAR are:

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

The 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). These standard deals exclusively with after-the-fact reporting.

The DSR SDT has consolidated disturbance and sabotage 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:

- Requires reporting of "events" that impact or may impact the reliability of the bulk electric system
- Provides clear criteria for reporting
- Includes consistent reporting timelines
- Identifies appropriate applicability, including a reporting hierarchy in the case of disturbance reporting
- Provides clarity around of who will receive the information

Discussion of Disturbance Reporting

Disturbance reporting requirements existed in the previous version of 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 were in the previous EOP-004 standard and its attachments. The DSR SDT discussed the reliability needs for disturbance reporting and developed the list of events that are to be reported under this standard (attachment 1).

Discussion of Event Reporting
There are situations worthy of reporting because they have the potential to impact reliability.

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

Examples of such 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 by reporting material risks to the Bulk Electrical System using the event categorization in this standard, it will be easier to get the relevant information for mitigation, awareness, and tracking, while removing the distracting element of motivation.

Certain types of 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 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. The standard requires Functional entities to report the incidents and provide known information at the time of the report. Further data gathering necessary for event analysis is provided for under the Events Analysis Program and the NERC

Rules of Procedure. 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 DSR SDT recognizes that some regions require reporting of additional information beyond what is in EOP-004. The DSR SDT has updated the listing of reportable events in Attachment 1 based on discussions with jurisdictional agencies, NERC, Regional Entities and stakeholder input. There is a possibility that regional differences still exist.

The reporting required by this standard 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 should not be 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.