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)
7. Third Comment Period and Initial Ballot (October 28 – December 12, 2011)
8. Fourth Comment Period and Successive Ballot (April 25 – May 24, 2012).

Proposed Action Plan and Description of Current Draft

This is the fifth posting of the proposed standard in accordance with Results-Based Criteria. The drafting team requests posting for a 30-day formal comment period concurrent with the formation of the ballot pool and the successive ballot.

Future Development Plan

Anticipated Actions	Anticipated Date
Drafting team considers comments, makes conforming changes on fourth posting	June - August 2012
Fourth Comment/Ballot period	August - September 2012
Recirculation Ballot period	October 2012
Receive BOT approval	November 2012
File with regulatory authorities	December 2012

Effective Dates

~~EOP-004-2 shall become effective on t~~The first day of the first ~~third~~ calendar quarter that is six months beyond the date that this standard is approved by ~~after~~ applicable regulatory authorities~~pproval~~. In those jurisdictions where no regulatory approval is required, this standard shall become effective on the first day of the first ~~third~~ calendar quarter that is six months beyond the date this standard is approved by the ~~after~~ NERC Board of Trustees ~~approval~~, or as otherwise made effective pursuant to the laws applicable to such ERO governmental authorities.

Version History

Version	Date	Action	Change Tracking
2		Merged CIP-001-2a Sabotage Reporting and EOP-004-1 Disturbance Reporting into EOP-004-2 Event Reporting; Retire CIP-001-2a Sabotage Reporting and Retired EOP-004-1 Disturbance Reporting. Retire CIP-008-3, 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 the reliability of the Bulk Electric System by requiring the reporting of events by Responsible Entities.

4. Applicability

4.1. Functional Entities: Within the context of EOP-004-2, the term "Responsible Entity" shall include the following entities as shown in EOP-004 Attachment 1:

4.1.1. Reliability Coordinator

4.1.2. Balancing Authority

~~**4.1.3. Interchange Coordinator**~~

~~**4.1.4. Transmission Service Provider**~~

~~**4.1.5.**~~**4.1.3. Transmission Owner**

~~**4.1.6.**~~**4.1.4. Transmission Operator**

~~**4.1.7.**~~**4.1.5. Generator Owner**

~~**4.1.8.**~~**4.1.6. Generator Operator**

~~**4.1.9.**~~**4.1.7. 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 Electric 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 EOP-004 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 EOP-004 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. EOP-004 Attachment 1 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. EOP-004 Attachment 1 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 EOP-004 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 Electric System 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.~~

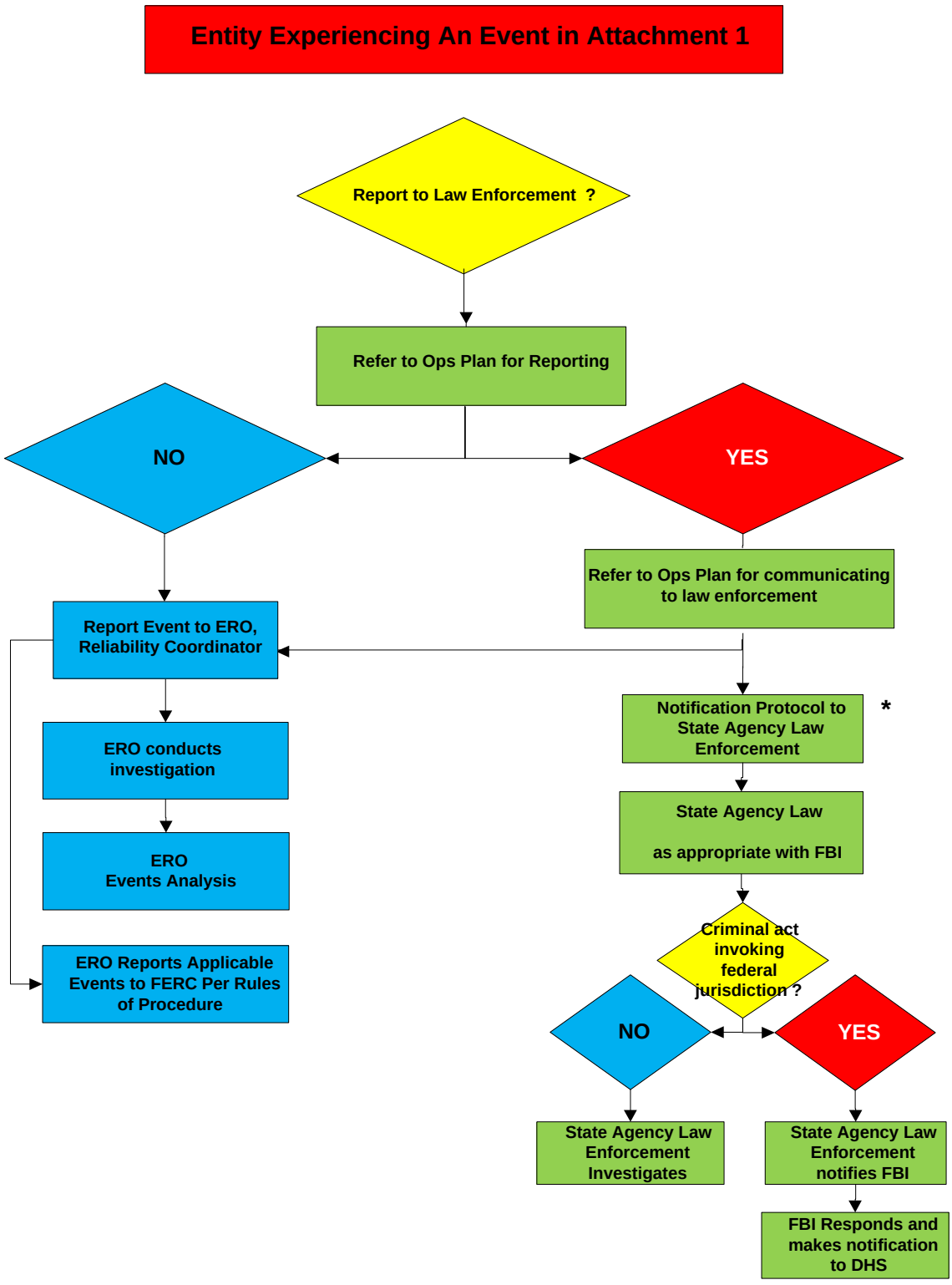
~~**Coordination of Local and Provincial Law Enforcement Agencies with the RCMP**~~

~~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.~~

Example of Reporting Process including Law Enforcement



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

B. Requirements and Measures

R1. Each Responsible Entity shall have an event reporting Operating Plan in accordance with EOP-004-2 Attachment 1 that includes the protocol(s) for reporting to the Electric Reliability Organization and other organizations (e.g., the regional entity, company personnel, the Responsible Entity's Reliability Coordinator, law enforcement, or governmental authority).~~that includes:~~ *[Violation Risk: Factor: Lower] [Time Horizon: Operations Planning]*

~~1.1. A process for recognizing each of the applicable events listed in EOP-004 Attachment 1(except for Cyber Security Incidents characterized and classified according to the requirements in CIP-008-3 or its successor).~~

~~1.2. A process for communicating each of the applicable events listed in EOP-004 Attachment 1 in accordance with the timeframes specified in EOP-004 Attachment 1 to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies.~~

Rationale for R1

The requirement to have an Operating Plan for reporting specific types of events provides the entity with a method to have its operating personnel recognize events that affect reliability and to be able to report them to appropriate parties; i.e. Regional Entities, applicable Reliability Coordinators, and law enforcement and other jurisdictional agencies when so recognized. In addition, these event reports are an input to the NERC Events Analysis Program. These other parties use this information to promote reliability, develop a culture of reliability excellence, provide industry collaboration and promote a learning organization.

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.

~~Part 1.1 clarifies that entities must address each of the "applicable" events listed in EOP-004 Attachment 1. Not all responsible entities must address all events; e.g., some events are only applicable to the Reliability Coordinator. Part 1.1 acknowledges that Cyber Security Incidents are characterized and classified according to the requirements in CIP-008-3.~~

~~Part 1.2~~The protocol(s) 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 contact information.

An existing procedure that meets the requirements of CIP-001-2a may be included in this Operating Plan along with other processes, procedures or plans to meet this requirement.

M1. Each Responsible Entity will have a current, dated, event reporting Operating Plan that includes, but is not limited to the protocol(s)~~, thresholds for reporting,~~ and each organization identified to receive an event report for event types specified in EOP-004-2 Attachment 1 and in accordance with the entity responsible for reporting~~which includes Parts 1.1 – 1.2~~.

R2. Each Responsible Entity shall report ~~implement its~~ events per their ~~reporting~~ Operating Plan within 24 hours of meeting an event type threshold for reporting~~for applicable events listed in EOP-004 Attachment 1, and in accordance with the timeframe specified in EOP-004 Attachment 1~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Assessment]*

M2. Each Responsible Entity will have as evidence of reporting an event, copy of the completed EOP-004-2 Attachment 2 form or a DOE-OE-417 form; and evidence of submittal (e.g., operator log or other operating documentation, voice recording, electronic mail message, or confirmation of facsimile) demonstrating the event report was submitted within 24 hours of meeting the threshold for reporting~~, for each event experienced, a dated copy of the completed EOP-004 Attachment 2 form or DOE form OE-417 report submitted for that event; and dated and time-stamped transmittal records to show that the event was reported supplemented by operator logs or other operating documentation. Other forms of evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other operating documentation for situations where filing a written report was not possible~~. (R2)

R3. Each Responsible Entity shall validate all contact information contained in the Operating Plan pursuant to Requirement R1 each calendar year~~conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2~~. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

Rationale for R2

Each Responsible Entity must report and communicate events according to its Operating Plan after the fact based on the information in EOP-004 Attachment 1. By implementing the event reporting Operating Plan, the Responsible Entity will assure situational awareness to the Electric Reliability Organization and other organizations needed for the event type; i.e. the Regional Entity; company personnel; the Responsible Entity's Reliability Coordinator; law enforcement, governmental or provincial agencies as deemed necessary by the Registered Entity. By communicating events per the Operating Plan, the Responsible Entity will assure that people/agencies are aware of the current situation and they may prepare to mitigate current and further events.

Rationale for R3 ~~and R4~~

Requirement~~s~~ 3 ~~and 4~~ call~~s~~ for the Responsible Entity to validate the contact information contained in the Operating Plan each calendar year. This requirement helps ensure that the event reporting Operating Plan is up to date and entities will be able to effectively report events to assure situational awareness to the Electric Reliability Organization. If an entity experiences an actual event, communication evidence from the event may be used to show compliance with the validation requirement for the specific contacts used for the event~~annual test of the communications process in Part 1.2 as well as an annual review of the event reporting Operating Plan. These two requirements help ensure that the event reporting Operating Plan is up to date and entities will be effective in reporting events to assure situational awareness to the Electric Reliability Organization and their Reliability Coordinator . This will assure that the BES remains secure and stable by mitigation actions that the Reliability Coordinator has within its function~~.

M3. Each Responsible Entity will have dated records to show that it validated all contact information contained in the Operating Plan each calendar year. Such evidence may include, but are not limited to, dated voice recordings and operating logs or other communication documentation~~and time-stamped records to show that the annual test of Part 1.2 was conducted. Such evidence may include, but are not limited to, dated and time stamped voice recordings and operating logs or other communication documentation. The annual test requirement is considered to be met if the responsible entity implements the communications process in Part 1.2 for an actual event~~. (R3)

~~**R4.** Each Responsible Entity shall conduct an annual review of the event reporting Operating Plan in Requirement R1. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*~~

~~**M4.** Each Responsible Entity will have dated and time-stamped records to show that the annual review of the event reporting Operating Plan was conducted. Such evidence may include, but are not limited to, the current document plus the 'date change page' from each version that was reviewed. (R4)~~

C. Compliance

1. Compliance Monitoring Process

1.1 Compliance Enforcement Authority

The Regional Entity shall serve as the Compliance E~~e~~nforcement Aauthority (CEA) unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional ~~e~~Entity approved by FERC or other applicable governmental authority shall serve as the CEA.

~~For NERC, a third-party monitor without vested interest in the outcome for NERC shall serve as the Compliance Enforcement Authority.~~

1.2 Evidence Retention

The [responsible entity] shall keep data or evidence to show compliance as identified below unless directed by its Compliance Enforcement Authority to retain specific evidence for a longer period of time as part of an investigation:
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 Operating Plan plus each version issued since the last audit for Requirements R1, and Measure M1.
- Each Responsible Entity shall retain evidence of compliance since the last audit for Requirements R2, R3 and Measure M2, M3.

~~Each Responsible Entity shall retain the current, document plus the 'date change page' from each version issued since the last audit for Requirements R1, R4 and Measures M1, M4.~~

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

If a Registered Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved 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 Audit
Self-Certification
Spot Checking
Compliance Investigation
Self-Reporting
Complaint

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	Operations Planning	Lower	N/A	N/A	~~The Responsible Entity has an event reporting Operating Plan but failed to include one of Parts 1.1 through 1.2.~~N/A	The Responsible Entity failed to include both Parts 1.1 and 1.2.
R2	Operations Assessment	Medium	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 24 hours but less than or equal to 36 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 36 hours but less than or equal to 48 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 48 hours but less than or equal to 60 hours after meeting an event threshold for reporting ~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to three entities identified	The Responsible Entity submitted a report (e.g., written or verbal) to all required recipients more than 60 hours after meeting an event threshold for reporting~~an event requiring reporting within 24 hours in EOP-004 Attachment 1~~. OR The Responsible Entity failed to submit an event report (e.g., written or verbal) to four or more entities identified in its event

			submitted an event report (e.g., written or verbal) to one entity identified in the event report Operating Plan within 24 hours. ~~in the appropriate timeframe but failed to provide all of the required information.~~	two entities identified in its event reporting Operating Plan within 24 hours..~~The Responsible Entity submitted a report more than 1 hour but less than 2 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~	in its event reporting Operating Plan within 24 hours.~~The Responsible Entity submitted a report in more than 2 hours but less than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~	reporting Operating Plan within 24 hours.~~The Responsible Entity submitted a report more than 3 hours after an event requiring reporting within 1 hour in EOP-004 Attachment 1.~~ OR The Responsible Entity failed to submit a report for an event in EOP-004 Attachment 1.
R3	Operations Planning	Medium	The Responsible Entity validated all contact information contained in the Operating Plan but was late by less than one calendar month. OR The Responsible Entity validated 75% or more of the contact information contained in the Operating Plan. ~~The Responsible Entity performed the annual test of the~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by one calendar month or more but less than two calendar months. OR The Responsible Entity validated 50% and less than 75% of the contact information contained in the Operating Plan.~~The Responsible Entity~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by two calendar months or more but less than three calendar months. OR The Responsible Entity validated 25% and less than 50% of the contact information contained in the Operating Plan. ~~The Responsible Entity~~	The Responsible Entity validated all contact information contained in the Operating Plan but was late by three calendar months or more. OR The Responsible Entity validated less than 25% of contact information contained in the Operating Plan. ~~The Responsible Entity performed the annual test of the~~

			communications process in Part 1.2 but was late by less than one calendar month.	performed the annual test of the communications process in Part 1.2 but was late by one calendar month or more but less than two calendar months.	performed the annual test of the communications process in Part 1.2 but was late by two calendar months or more but less than three calendar months.	communications process in Part 1.2 but was late by three calendar months or more. OR The Responsible Entity failed to perform the annual test of the communications process in Part 1.2.
R4	Operations Planning	Medium	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by less than one calendar month.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by one calendar month or more but less than two calendar months.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by two calendar months or more but less than three calendar months.	The Responsible Entity performed the annual review of the event reporting Operating Plan but was late by three calendar months or more. OR The Responsible Entity failed to perform the annual review of the event reporting Operating Plan

D. Variances

None.

E. Interpretations

None.

F. References~~Interpretations~~

Guideline and Technical Basis (attached).

EOP-004 - Attachment 1: Reportable Events

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 Requirement R1 and provide as much information as is available at the time of the notification. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net or Voice: 404-446-9780.~~esisac@nerc.com, Facsimile: 609-452-9550, Voice: 609-452-1422~~.

~~**One Hour Reporting: Submit EOP-004 Attachment 2 or DOE-OE-417 report to the parties identified pursuant to Requirement R1, Part 1.2 within one hour of recognition of the event.**~~

~~Event~~	~~Entity with Reporting Responsibility~~	~~Threshold for Reporting~~
~~A reportable Cyber Security Incident.~~	~~Each Responsible Entity applicable under CIP-008-3 or its successor that experiences the Cyber Security Incident~~	~~That meets the criteria in CIP-008-3 or its successor~~

Rationale Box for EOP-004 Attachment 1:

The DSR SDT used the defined term “Facility” to add clarity for several events listed in Attachment 1. A Facility is defined as:

> “A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)”

The DSR SDT does not intend the use of the term Facility to mean a substation or any other facility (not a defined term) that one might consider in everyday discussions regarding the grid. This is intended to mean ONLY a Facility as defined above.

~~Twenty-four Hour Reporting:~~ Submit EOP-004 Attachment 2 or DOE-OE-417 report ~~to the parties identified~~ pursuant to Requirements R1 and R2~~, Part 1.2 within twenty-four hours of recognition of the event~~.

Event	Entity with Reporting Responsibility	Threshold for Reporting
Damage or destruction of a Facility	~~Each~~ RC, BA, TO~~, TO~~P~~, GO, GOP, DP that experiences the damage or destruction of a Facility~~	Damage or destruction of a Facility within its Reliability Coordinator Area, Balancing Authority Area or Transmission Operator Area that results in actions to avoid a BES Emergency.~~Damage or destruction of a Facility that:~~ ~~Affects an IROL (per FAC-014)~~ ~~OR~~ ~~Results in the need for actions to avoid an Adverse Reliability Impact~~ ~~OR~~ ~~Results from actual or suspected intentional human action.~~
Damage or destruction of a Facility	BA, TO, TOP, GO, GOP, DP	Damage or destruction of its Facility that results from actual or suspected intentional human action.
~~Any p~~Physical threats to ~~that could impact the operability of~~ a Facility[1]	~~Each RC,~~ BA, TO, TOP, GO, GOP, DP ~~that experiences the event~~	Physical threat to its Facility excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the Facility. OR Suspicious device or activity at a Facility. Do not report theft unless it degrades normal operation of a

[1] ~~Examples include a train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center). Also report any suspicious device or activity at a Facility. Do not report copper theft unless it impacts the operability of a Facility.~~

Event	Entity with Reporting Responsibility	Threshold for Reporting
		Facility.~~Threat to a Facility excluding weather related threats.~~
Physical threats to a BES control center	RC, BA, TOP	Physical threat to its BES control center, excluding weather or natural disaster related threats, which has the potential to degrade the normal operation of the control center. OR Suspicious device or activity at a BES control center.
BES Emergency requiring public appeal for load reduction	Initiating entity is responsible for reporting	Public appeal for load reduction event
BES Emergency requiring system-wide voltage reduction	Initiating entity is responsible for reporting	System wide voltage reduction of 3% or more
BES Emergency requiring manual firm load shedding	Initiating entity is responsible for reporting	Manual firm load shedding ≥ 100 MW
BES Emergency resulting in automatic firm load shedding	~~Each~~ DP~~, or~~ TOP ~~that implements automatic load shedding~~	Automatic f~~F~~irm load shedding ≥ 100 MW (via automatic undervoltage or underfrequency load shedding schemes, or SPS/RAS)
Voltage deviation on a Facility	~~Each~~ TOP ~~that observes the voltage deviation~~	Observed within its area a voltage deviation of ± 10% sustained for ≥ 15 continuous minutes
IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only)	~~Each~~ RC ~~that experiences the IROL Violation (all Interconnections) or SOL violation for Major WECC Transfer Paths (WECC only)~~	Operate outside the IROL for time greater than IROL T_v (all Interconnections) or Operate outside the SOL for more than 30 minutes for Major WECC Transfer Paths (WECC only).
Loss of firm load ~~for ≥ 15 Minutes~~	~~Each~~ BA, TOP, DP ~~that experiences the loss of firm load~~	Loss of firm load for ≥ 15 Minutes: • ≥ 300 MW for entities with previous year's demand ≥ 3,000 MW • ≥ 200 MW for all other entities

Event	Entity with Reporting Responsibility	Threshold for Reporting
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
Generation loss	~~Each~~ BA, GOP ~~that experiences the generation loss~~	Total generation loss, within one minute, of ≥ 2,000 MW for entities in the Eastern or Western Interconnection OR ≥ 1,000 MW for entities in the ERCOT or Quebec Interconnection
Complete loss of off-site power to a nuclear generating plant (grid supply)	~~Each~~ TO, TOP ~~that experiences the complete loss of off-site power to a nuclear generating plant~~	Complete loss of off-site power a~~A~~ffecting a nuclear generating station per the Nuclear Plant Interface Requirement
Transmission loss	~~Each~~ TOP ~~that experiences the transmission loss~~	Unexpected loss, contrary to design, of three or more BES Elements caused by a common disturbance ~~Unintentional loss of three or more Transmission Facilities~~ (excluding successful automatic reclosing)
Unplanned control center evacuation	~~Each~~ RC, BA, TOP ~~that experiences the event~~	Unplanned evacuation from BES control center facility for 30 minutes or more.
Complete ~~L~~loss of ~~all~~ voice communication capability	~~Each~~ RC, BA, TOP ~~that experiences the loss of all voice communication capability~~	Complete loss of voice communication capability a~~A~~ffecting a BES control center for ≥ 30 continuous minutes
Complete ~~or partial~~ loss of monitoring capability	~~Each~~ RC, BA, TOP ~~that experiences the complete or partial loss of monitoring capability~~	Complete loss of monitoring capability a~~A~~ffecting a BES control center for ≥ 30 continuous minutes such that analysis tools (i.e., State Estimator or~~,~~ Contingency Analysis) are rendered inoperable.

EOP-004 - Attachment 2: Event Reporting Form

EOP-004 Attachment 2: Event Reporting Form **Use this form to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail:** systemawareness@nerc.net voice: 404-446-9780~~esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422~~**.**		
Task		**Comments**
1.	Entity filing the report include: Company name: Name of contact person: Email address of contact person: Telephone Number: Submitted by (name):	
2.	Date and Time of recognized event. Date: (mm/dd/yyyy) Time: (hh:mm) Time/Zone:	
3.	Did the event originate in your system?	Yes ☐ No☐ Unknown ☐
4.	**Event Identification and Description:**	
	(Check applicable box) ☐ Damage or destruction of a Facility ☐ Physical Threat to a Facility ☐ Physical Threat to a control center ☐ BES Emergency: ☐ public appeal for load reduction ☐ system-wide voltage reduction ☐ manual firm load shedding ☐ automatic firm load shedding ☐ Voltage deviation on a Facility ☐ IROL Violation (all Interconnections) or SOL Violation for Major WECC Transfer Paths (WECC only) ☐ Loss of firm load ☐ System separation ☐ Generation loss ☐ Complete loss of off-site power to a nuclear generating plant (grid supply) ☐ Transmission loss ☐ unplanned control center evacuation ☐ Complete loss of voice communication capability ☐ Complete loss of monitoring capability ~~(Check applicable box)~~ ~~☐ public appeal~~	Written description (optional):

EOP-004 Attachment 2: Event Reporting Form

Use this form to report events. The Electric Reliability Organization and the Responsible Entity's Reliability Coordinator will accept the DOE OE-417 form in lieu of this form if the entity is required to submit an OE-417 report. Submit reports to the ERO via one of the following: e-mail: systemawareness@nerc.net voice: 404-446-9780~~**esisac@nerc.com, Facsimile: 609-452-9550, voice: 609-452-1422**~~**.**

Task		Comments
	☐ ~~voltage reduction~~ ☐ ~~manual firm load shedding~~ ☐ ~~firm load shedding(undervoltage, underfrequency, SPS/RAS)~~ ☐ ~~voltage deviation~~ ☐ ~~IROL violation~~ ☐ ~~loss of firm load~~ ☐ ~~system separation (islanding)~~ ☐ ~~generation loss~~ ☐ ~~complete loss of off-site power to nuclear generating plant~~ ☐ ~~transmission loss~~ ☐ ~~damage or destruction of Facility~~ ☐ ~~unplanned control center evacuation~~ ☐ ~~loss of all voice communication capability~~ ☐ ~~complete or partial loss of monitoring capability~~ ☐ ~~physical threat that could impact the operability of a Facility~~ ☐ ~~reportable Cyber Security Incident~~	

Guideline and Technical Basis

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 EOP-004 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 EOP-004 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. EOP-004 Attachment 1 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. EOP-004 Attachment 1 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 EOP-004 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 Electric System 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.

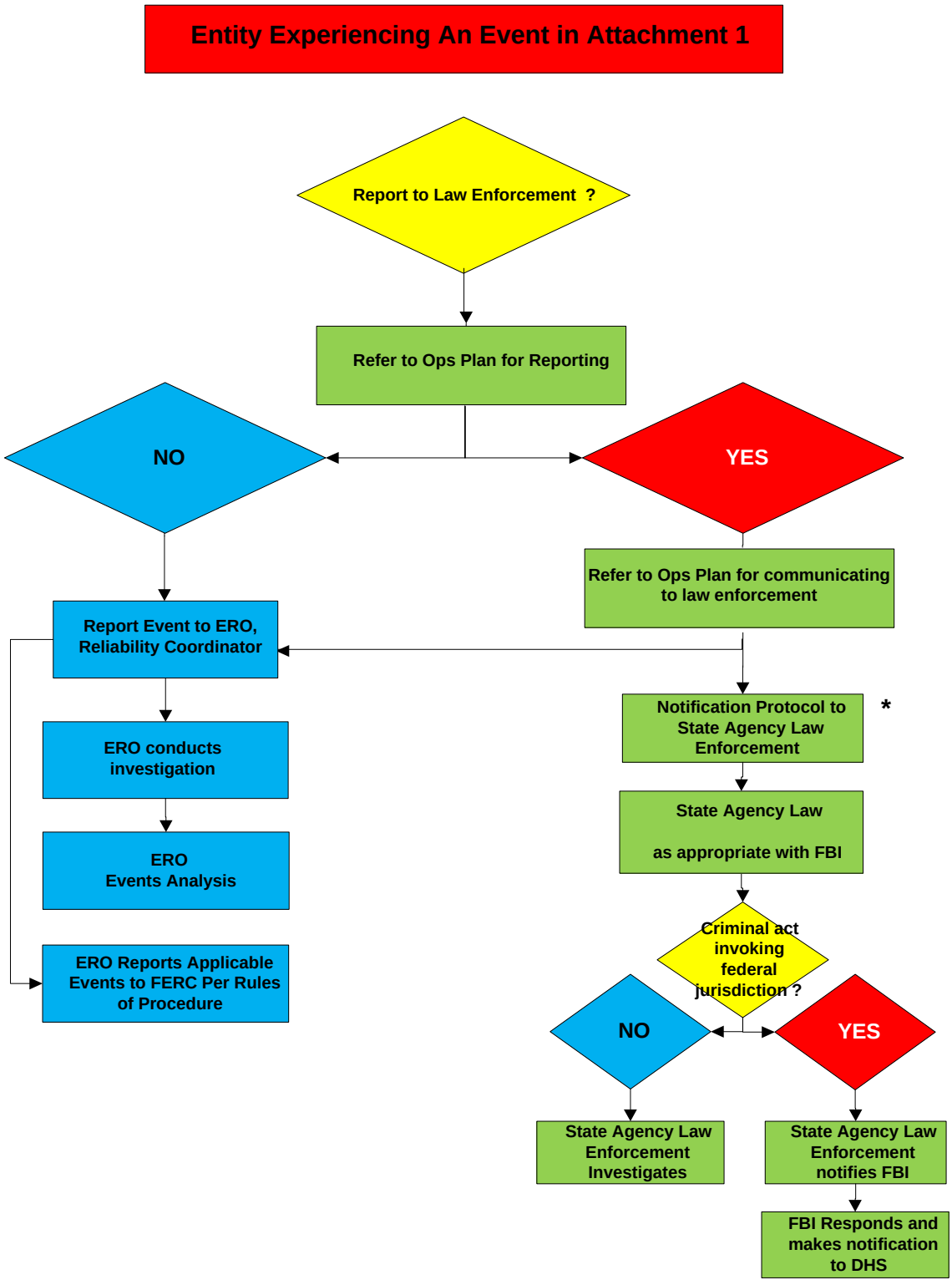
Coordination of Local and Provincial Law Enforcement Agencies with the RCMP

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.

Example of Reporting Process including Law Enforcement



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

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 (EOP-004 Attachment 1).

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

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-008-3 or its successor standard~~
- ~~Forced intrusion attempt at a substation~~
- Train derailment adjacent to a Facility that either could have damaged a Facility directly or could indirectly damage a Facility (e.g. flammable or toxic cargo that could pose fire hazard or could cause evacuation of a control center)~~near a transmission right-of-way~~
- Destruction of Bulk Electric 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 Electric 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 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 EOP-004 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.