

**Project 2009-01 Disturbance and Sabotage Reporting Comment Received
April 29, 2009 through May 13, 2009**

- Individual or group. (40 Responses)**
- Name (28 Responses)**
- Organization (28 Responses)**
- Group Name (12 Responses)**
- Contact Organization (12 Responses)**
- Question 1 (39 Responses)**
- Question 1 Comments (40 Responses)**
- Question 2 (40 Responses)**
- Question 2 Comments (40 Responses)**
- Question 3 (38 Responses)**
- Question 3 Comments (40 Responses)**
- Question 4 (39 Responses)**
- Question 4 Comments (40 Responses)**
- Question 5 (0 Responses)**
- Question 5 Comments (40 Responses)**

Individual
Stephen V. Fisher
Lands Energy Consulting
Yes
I have worked with 5 Northwest public utilities on developing procedures related to CIP-001-1 and EOP-004-1. All 5 utilities operate electric systems in fairly remote locations and are embedded in a larger utility's Balancing Authority/Transmission Operator area. A. CIP-001-1 - Developing procedures to unambiguously identify acts of sabotage has been particularly challenging for these systems. In general, it's hard for them to determine whether the most prevalent forms of malicious and intentional system damage that they incur - copper theft and gun shot insulators/equipment - should qualify as acts of sabotage. Although none of the systems consider copper theft to be acts of sabotage, two of the systems consider gun shot insulators/equipment to be acts of sabotage. The other systems look for intent to disrupt electric system operations as a key component of their sabotage identification procedures. Additional guidance from NERC in the form of CIP-001-1 modifications or a companion guidelines document on sabotage identification would provide much needed guidance for these procedures. B. EOP-004-1 - This standard was clearly drafted with the larger electric systems in mind. I have one client that serves 3300 commercial/residential customers from 4-115/13 kV substation transformers and one large industrial customer (80% of its energy load) from a 230/13 kV substation. 75% of the client's load is served from three substations attached to a long, 115 kV transmission line operated by the Bonneville Power Administration. Whenever the line relays open on a permanent fault (which happens 2-3 times per year), the client loses over 50% of its customers (but no more than 10-15 MW during winter peak), thereby necessitating the preparation of a Disturbance Report. To allow utilities to concentrate on operating their systems, without fear of violating EOP-004-1 for failure to report trivial outages, I would remove LSEs from the obligation to report disturbances - leave the reporting to the BA/TOP for large outages in their footprint.
No
I would like to see the SAR expanded to cover the issues I mentioned in my prior comment. Otherwise, the scope of the SAR looks fine to me.
No
No
CIP-001-1 - Yes. In many cases, the staff of an LSE embedded in another entity's BA/TOP area is more

likely to discover an act of sabotage directed toward a BA/TOP-owned facility that could affect the BES than the asset owner. This is because the LSE likely has more operating staff in the area. I have included a requirement in my clients' Sabotage Identification and Reporting Procedures that the client treat acts of sabotage to a third party's system discovered by client employees as though the act was directed toward client facilities. EOP-004-1 - As mentioned before, I would eliminate the LSE from the applicability list and leave the responsibility for disturbance reporting and response to the TOP/BA. However, I would retain a responsibility for the LSEs to cooperate (when requested) with any disturbance investigation.

One final comment on CIP-001-1. My clients received universally rude treatment from the FBI field offices when they attempted to establish the contacts required by the Standard. If the FBI doesn't see value in establishing these contacts, remove the requirement from the Standard. Making sure the LSE knows the FBI field office phone number is probably all the Standard should require.

Individual

Brent Hebert

Calpine Corporation

Yes

Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA, GOP, or LSE in which the facility resides should be coordinated for EOP -004 reporting. The reporting to NERC/DOE should come from the RC, BA, GOP, or LSE.

Yes

No

The reporting requirements of EOP - 004 are needed for the RC, BA, LSE and the GOP that operates or controls generation in a system as defined by NERC. (System – A combination of generation, transmission, and distribution components). A disturbance is described as an unplanned event that produces and abnormal system condition, any perturbation to the electric system, and the unexpected change in ACE that is caused by the sudden failure of generation or interruption of load. The GOP operating/controlling generation within a system has the ability to analyze system conditions to determine if reporting is necessary. A NERC registered GOP that is a merchant generator within another company's system does not have the ability for a wide area view and cannot analyze system conditions beyond the interconnection point of the facility. Moreover, in most cases the reporting requirements outlined in the Interconnection Reliability Operating Limits and Preliminary Disturbance Report do not apply to the merchant generator that is not a generation only BA. The applicability of the standard does encompass the true merchant generation entities required to register as GOP. Similarly, the OE-417 table 1 reporting requirements generally do not apply to a true merchant generating entity that is required to register as a GOP.

Individual

Steve Toth

Covanta

Yes

Yes - the key to Sabotage reporting requirements is identifying what the 'definition' is of an actual or potential 'Sabotage' event. Like any other standard, if FERC/NERC leave it up to 2000+ entities to establish their own definitions of 'Sabotage', you may likely get 2000+ answers. That is not a controlled and coordinated approach. I offer the following definition, "Sabotage - Deliberate or malicious destruction of property, obstruction of normal operations, or injury to personnel by outside agents." Examples of sabotage events could include, but are not limited to, suspicious packages left near site electrical generating or electrical transmission assets, identified destruction of generating assets, telephone/e mail received threats to destroy or interrupt electrical generating efforts, etc." These have passed multiple NERC regional audits and reviews to date.

Yes

No
Yes
It would be a welcome enhancement to the end users to understand to communication link between all "appropriate parties" who shall be notified of potential or actual sabotage events.... which also needs to be defined.
Individual
Harvie Beavers
Colmac Clarion
Yes
Yes
No
Yes
Need single report for Sabotage so whatever is required results in notification of all parties (State Emergency Management, Homeland Security, FBI, Grid Reliability Chain of Command). Any and all of these can 'expand' knowledge later but all seem to require 'instant' notification.
Individual
Russell A. Noble
Cowlitz County PUD
Yes
The standards as written now create reporting on local customer quality of service outage events not related to BPS disturbances. Sabotage reporting has degenerated into reporting of mischievous vandalism and minor theft occurrences. This creates compliance documentation overburden and waste of limited funds needed for true BPS reliability concerns, and also adds nuisance calls to the FBI and Homeland Security.
No
Added to the scope: For EOP-004 add a provision for a reporting flow rather than everything going to the RE and NERC, that is something going like the DP and TOP reports to the BA, the BA to the RE, and the RE to NERC. This would allow for multiple related reports to be combined into a single coherent report as the reporting goes up the chain. For CIP-001 consider reporting flow as above with local law enforcement notification. Let an upper entity in the reporting chain decide when to contact Federal Agencies such as the BA or the RC.
No
No
Replace LSE with DP, and the Regional Reliability Organization with the Regional Entity.
Local Law enforcement agencies often are not friendly to Federal involvement with smaller problems they consider their "turf." Need to make sure the small stuff stays with them, however have a system of internal reporting that will catch coordinated sabotage efforts (multiple attacks on DPs and small BAs) at the RC or RE level who then can report to the Federal agencies. Currently EOP-004-1 requires small entities to report a "disturbance" if half of their firm customer load is lost. For some entities, this can be one small substation going down due to a bird. The "50% of total demand" requirement should be removed or improved to better define a true BPS disturbance.
Individual
Michael Puscas

United Illuminating
Yes
Yes
No
No
Add Distribution Provider
Individual
George Pettyjohn
Reliant Energy
Yes
EOP-004-1 indicates that Generators should analyze disturbances on the bulk electrical system or their facilities. Generators do not have the capability of analyzing the bulk electrical system other than Frequency. Even so, generators can not unilaterally respond to what it thinks are disturbances. In the case of CAISO The Participating Generator Agreement prevents me from making any unilateral moves save for the direct frequency emergencies. If the System operator or Reliability Coordinator informs the generator that there is a disturbance and that logs and readouts etc. are required then the generator should respond with all available information for the subject hours or time. Clearer responsibilities provide clearer results.
No
I think Generator operators should be excluded except to provide requested information from the System Operator or Reliability coordinator.
No
No
EOOP-004-1 should exclude the generator operator from disturbance reporting except providing the system operator or reliability coordinator with appropriate unit operation information upon request. Acts of sabotage should be identified clearly and reported to the indicated authorities.
Individual
Judith A. James
Texas Regional Entity
Yes
Yes
No
No
Add GO and TO to the list of applicability. The intent of CIP-001-1 when it was first written was to have the proper and most likely entities associated directly with operations to be the ones to begin the reporting process in the case of sabotage on the system. In the ERCOT Region and other regions in the US, the GOP may not be physically located at the site. The GOP is often removed from the minute-by-minute responsibilities of plant operations and, therefore, may be less able to react to physical sabotage at the location/plant/facility in a timely manner. The concern is that, in the case of an actual sabotage event, the failure to report to the appropriate authorities in a timely manner may jeopardize the reliability of the BPS. Therefore, the Generator Owner (GO) should be added to the list of applicability for CIP-001-1, because it is

the GO that is more likely to be on location at the generation site and thus aware of sabotage when it first occurs. This would disallow for any possible communication gap and put responsibility on all of the appropriate entities to report such an event. Additionally, and for the same reasons as adding the GO, the Transmission Owner (TO) should also be added to the list of applicability for reporting sabotage on its facilities.

Individual

Edward C. Stein

self

Yes

Yes

No

Yes

Individual

Chris Scanlon

Exelon

Yes

Yes

Consolidation of redundant requiremnts and clarifications of difficult to follow / interpret standards should be a high priority at NERC.

No

We are not sure what this question means. Who's Associated Business practices, NERC, Applicable Entities in the Standard, our business practices?

No

CIP-001, remove LSE's from the standard for the reasons identified in the FERC LSE order. Ad TO and DP. EOP-004, remove LSE's from the standard for the reasons identified in the FERC LSE order. Remove RRO's, they are not a user, owner, operator of the BES. Add DP or TO. Consider conditional applicability as in the UFLS standards, " the TO or DP who performs the functions specified in the standard..."

Exelon agrees this is a worthwhile project and that reliability will be enhanced and the compliance process will be simplified by clarifying terminology and reporting requirements in these standards. If nothing else, defining "Sabotage" so as to end interpretations of this term and the related requirements is necessary.

Group

SERC OC Standards Review Group

Entergy Services, Inc

No

The EOP-004-1 standard is an unnecessary duplication of existing DOE reporting requirements. This essentially exposes an entity to fines by NERC, enforced by FERC, for failure to comply with a DOE regulation, which seems improper to us. In addition, reporting requirements do not have an impact on the reliability of the BES

Yes

No

Business practices should not be considered in a standard.
No
The EOP-004-1 standard should not apply to the RRO.
Group
WECC
WECC
Yes
Yes
No
Yes
No
Group
Project 2007-02 Operating Personnel Comms Protocols SDT
NERC OPCP SDT
No
The Operating Personnel Communication Protocols standard drafting team respectfully requests that the Sabotage Reporting SAR Drafting Team incorporate the following into your proposed SAR: "Each Reliability Coordinator, Balancing Authority, and Transmission Operator shall have procedures for the communication of information concerning the Cyber and Physical emergency alerts in accordance with the conditions described in Attachment 1 Security Emergency Alerts ." The Operating Personnel Communications Protocols Project 2007-02 was initiated to ensure that real time system operators use standardized communication protocols during normal and emergency operations to improve situational awareness and shorten response time. The SDT developed a new COM-003-1 Standard that has yet to be posted and is dependent upon revising at least two other standards (CIP-001 and TOP Standard). COM-003 contains requirements that specify: 1. Use of three-part communication; 2. English language; 3. Common time zone; 4. NATO alpha-numeric alphabet; 5. Mutually agreed line identifiers; 6. The use of pre-defined system condition terminology such as those contained in the RCWG Alert Level Guide and EOP-002-2. This request is based on recent NERC Standards Committee direction to our team to incorporate the Reliability Coordinator Working Group's (RCWG) Alert Level Guide into a Standard. The consensus of our team is that a TOP Standard is the most appropriate location for the Transmission Emergency Alert language from the Guide as the energy emergency alert language is currently described in EOP-002-2. The RCWG Guide proposes the use of pre-defined system condition descriptions for use during emergencies for reliability related information. This guide was developed in response to a Blackout Report recommendation. Our team placed the Transmission Emergency Alert language into a TOP standard. Since the Sabotage Reporting SAR DT intends to modify CIP-001, we seek your consent to incorporate the cyber and physical security alert language to comply with the wishes of the Standards Committee. We believe that the CIP-001 Standard is the most appropriate location for this language for the following reasons: • The levels of emergency conditions related to the cyber and physical security of the electric system is directly related to Critical Infrastructure Protection. • The current version of CIP-001 already requires the timely reporting of actual and suspected security emergency conditions and the use of pre-defined terminology supports the efficient sharing of such information. The OPCP SDT includes the following text for the record. It is a proposed draft revision of CIP-001. A. Introduction 1. Title: Security Incidents 2. Number: CIP-001-2 3. Purpose: To ensure the recognition, communication and response to cyber and physical security incidents suspected or determined to be caused by sabotage. 4. Applicability 4.1. Reliability Coordinators. 4.2. Balancing Authorities. 4.3. Transmission Operators. 4.4. Generator Operators. 4.5. Load Serving Entities. 5. Effective

Date: The standard is effective the first day of the first calendar quarter after applicable regulatory approvals (or the standard otherwise becomes effective the first day of the first calendar quarter after NERC BOT adoption in those jurisdictions where regulatory approval is not required).

B. Requirements R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of security threats on its facilities and multi site security threats affecting larger portions of the Interconnection.

R2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the communication of information concerning the physical and cyber security status of their facilities in accordance with the conditions described in Attachment 1-CIP-001-1.

R3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall provide its operating personnel with security threat or incident response guidelines, including personnel to contact, for reporting security threats and incidents.

R4. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall establish communications contacts, as applicable, with local Federal Bureau of Investigation (FBI) or Royal Canadian Mounted Police (RCMP) officials and develop reporting procedures as appropriate to their circumstances.

C. Measures M1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request a procedure (either electronic or hard copy) as defined in Requirement 1

M2. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request the procedures or guidelines that will be used to confirm that it meets Requirements 2 and 3.

M3. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have and provide upon request evidence that could include, but is not limited to procedures, policies, a letter of understanding, communication records, or other equivalent evidence that will be used to confirm that it has established communications contacts with the applicable, local FBI or RCMP officials to communicate sabotage events (Requirement 4).

D. Compliance

1. Compliance Monitoring Process

1.1. Compliance Enforcement Authority Regional Entity

1.2. Compliance Monitoring Period and Reset One or more of the following methods will be used to verify compliance: - Compliance Audits - Self-certifications - Spot Checking - Compliance Violation Investigations - Self-Reporting - Complaints

1.3. Data Retention The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider 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:

- o The Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator and Distribution Provider shall retain its current, in force document and any documents in force since the last compliance audit.
- o If a Transmission Operator, Transmission Owner, Balancing Authority, Reliability Coordinator, Generator Operator or Distribution Provider is found non-compliant, it shall keep information related to the non-compliance until found compliant.
- o The Compliance Enforcement Authority shall keep the last audit records and all requested and submitted subsequent audit records.

1.4. Additional Compliance Information None.

2. Levels of Non-Compliance:

2.1. Level 1: There shall be a separate Level 1 non-compliance, for every one of the following requirements that is in violation:

- 2.1.1** Does not have procedures for the recognition of and for making its operating personnel aware of sabotage events (R1).
- 2.1.2** Does not have procedures or guidelines for the communication of information concerning sabotage events to appropriate parties in the Interconnection (R2).
- 2.1.3** Has not established communications contacts, as specified in R4.

2.2. Level 2: Not applicable.

2.3. Level 3: Has not provided its operating personnel with sabotage response procedures or guidelines (R3).

2.4. Level 4: .Not applicable.

E. Regional Differences None.

Version History

Version	Date	Action
0	April 1, 2005	Effective Date New
0	August 8, 2005	Removed "Proposed" from Effective Date
1	November 1, 2006	Adopted by Board of Trustees
1	April 4, 2007	Regulatory Approval — Effective Date New
2	March 2009	Added SEA attachment and updates to Effective Date and Compliance sections.

New Attachment 1-CIP-001-2 Physical Security Emergency Alerts General Requirements

1. Initiation by Reliability Coordinator. A Physical Security Emergency Alert may be initiated only by a Reliability Coordinator at:

- a. The Reliability Coordinator's own decision,
- b. By request from a Transmission Operator,
- c. By request from a Balancing Authority, or
- d. By request from federal, state, or local Law Enforcement Officials.

2. Situations for initiating alert. An Alert may be initiated for the following reasons:

- a. A physical threat affecting a control center, grid or generator asset has been identified, or
- b. A physical attack affecting a control center, grid or generator asset has occurred or is imminent.

3.

Notification. A Reliability Coordinator who initiates a Physical Security Emergency Alert shall notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the "CIP" category. Additionally, conference calls between Reliability Coordinators shall be held as necessary to communicate system conditions. The Reliability Coordinator shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended. Physical Security Emergency Alert Levels To ensure that all Reliability Coordinators clearly understand potential and actual Physical Security Emergency Alerts, NERC has established three levels of Security Emergency Alerts. The Reliability Coordinators will use these terms when explaining security alerts to each other. The Reliability Coordinator may declare whatever alert level is necessary, and need not proceed through the alerts sequentially.

1. Alert 1 – "Control Center / Bulk Electric System asset threat identified" Circumstances: A credible threat of physical attack on a Bulk Electric System asset has been communicated to the Reliability Coordinator. No physical attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered: a. The nature and specificity of the threat, b. The timing of the threat, c. Mode of threat communication, and d. The criticality of the threatened asset. During a Physical Security Emergency Alert Level 1, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities:
 - i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area.
 - ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the Reliability Coordinator of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.
2. Alert 2 – "Verified Physical attack at a single site" Circumstances: A Reliability Coordinator, Transmission Operator, or Balancing Authority has identified a physical attack upon a control center, generator asset, or other bulk electric system asset. During a Physical Security Emergency Alert Level 2, Reliability Coordinators, Transmission Operators and Balancing Authorities shall have the following responsibilities:
 - i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area.
 - ii. Updating Status during the Physical Security Emergency Alert The declaring Entity shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.
3. Alert 3 – "Verified Physical attack at multiple sites" Circumstances: Multiple attacks have been confirmed on control centers, generator assets or other bulk electric system assets. A Reliability Coordinator shall declare a Physical Security Emergency Alert 3 whenever:
 - a. A Transmission Operator or Balancing Authority reports multiple physical attacks on bulk electric system assets,
 - b. Multiple Transmission Operators or Balancing Authorities report one or more physical attacks on their bulk electric system assets.
 - i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area.
 - ii. Updating Status during the Physical Security Emergency Alert The declaring Entity(ies) shall update the Reliability Coordinator of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.
4. Alert 0 – "Termination of Alert Level" Circumstances: The threat which prompted the Physical Security Emergency Alert Level has diminished or has been removed.
 - i. Notification The Reliability Coordinator responsible for initiating the Physical Security Emergency Alert shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated.

Cyber Security Emergency Alerts
Cyber Assets – Those programmable electronic devices and communication networks, including hardware, software, and data, associated with bulk electric system assets.
Cyber Security Incident – Any malicious act or suspicious event that compromises, or attempts to compromise, the electronic or physical security perimeter of a critical cyber asset or disrupts or attempts to disrupt the operation of a critical cyber asset.
Critical Cyber Asset – Those cyber assets essential to the reliable operation of critical assets.
Electronic Security Perimeter – The logical border surrounding the network or group of sub-networks to which the critical cyber assets are connected, and for which access is controlled.
Physical Security Perimeter – The physical border surrounding computer rooms, telecommunications rooms, operations

centers and other locations in which critical cyber assets are housed and for which access is controlled.

General Requirements

1. Initiation - A Cyber Security Emergency Alert shall be initiated by:
 - a. The Reliability Coordinator's analysis,
 - b. By request from any NERC functional Model entity that Com-003-0 is applicable to.
 - c. By request from federal, state, or local Law Enforcement Officials.
2. Situations for initiating alert. An Alert shall be initiated for the following reasons:
 - a. A cyber threat affecting a control center or bulk electric system asset has been identified, or
 - b. A cyber attack affecting a control center or bulk electric system has occurred or is imminent.
3. Notification. An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall notify FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. The Reliability Coordinator shall also notify as necessary other Reliability Coordinators of the situation via the Reliability Coordinator Information System (RCIS) using the "CIP" category. The Reliability Coordinator shall notify all Transmission Operators and Balancing Authorities in its Reliability Area and other Reliability Coordinators when the alert has changed levels or ended.

Cyber Security Emergency Alert Levels To ensure that all applicable entities clearly understand potential and actual Cyber Security Emergency Alerts, three levels of Security Emergency Alerts shall be used. The Reliability Coordinators will use these terms when communicating security alerts to each other. When declaring the applicable alert level it is important to note that the applicable level can be determined without sequentially proceeding through levels. As an example given circumstances an Alert Level 3 could be called without previously being in an Alert Level 1 or Level 2 state.

1. Alert 1 – "Verified Control Center / Bulk Electric System Cyber Asset threat identified or imminent" What is "verified" - unknown or unauthorized access to a cyber device, unknown or unauthorized change to a cyber device (i.e., config file, O/S, firmware change. 'Verified' could mean the elimination of a false positive in your security monitoring system. 'Verified' could also be the differentiation between malicious and non-malicious (ie human error, not following policy, etc) intent. What is a "threat" - A threat can be perceived as any action or event that occurs where the monitoring authority was not previously made aware that that action would occur. With flimsy change control or access controls, field staff or technical staff performing troubleshooting or other maintenance may access or change devices without notifying the monitoring entity. The monitoring entity would have to treat this as a threat and take appropriate action to either isolate that device from the rest of the system, notify appropriate authority, dispatch a crew, etc Examples of threats - Over and above the examples above, another threat example could be a notification from DHS or other security agency that they have reason to believe a hack, virus or other cyber terrorism activity could occur. Also, noticing a distinct change in network traffic which could imply someone has intercepted your data and can manipulate it before sending it from the control room to the device being controlled or manipulating the data coming from the device before a controller seeing it and forcing them to perform an incorrect control event in reaction to erroneous data. Circumstances: A credible threat of Cyber attack on a Control Center or Bulk Electric System asset has been communicated to the Reliability Coordinator. No cyber attack has occurred at this point. Determining the credibility of any threat is a subjective process, but the following factors should be considered:
 - a. The nature and specificity of the threat,
 - b. The timing of the threat,
 - c. Mode of threat communication, and
 - d. The criticality of the threatened asset.During a Cyber Security Emergency Alert Level 1, applicable entities shall have the following responsibilities:
 - i. Notification An entity who initiates a Cyber Security Emergency Alert Level 1 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify as necessary the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security.
 - ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall update those applicable entities of any changes in the situation until the Alert Level 1 is terminated. The Reliability Coordinator shall update the RCIS as changes occur.
2. Alert 2 – "Verified Cyber attack on a Control Center or Bulk Electric System asset" Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset. During a Cyber Security Emergency Alert Level 2, applicable entities shall have the following responsibilities:
 - i. Notification An entity who initiates a Cyber Security Emergency Alert Level 2 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator responsible shall post the declaration of the alert level along with the location of the affected facility on the RCIS under "CIP" and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office,

Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity shall provide updates of the situation a minimum of once per hour until the Alert Level 2 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 3. Alert 3 – “Verified Cyber attack at one or more Control Center or Bulk Electric System cyber asset” Circumstances: An applicable entity has identified a cyber attack upon a control center or bulk electric system asset and shall declare a Cyber Security Emergency Alert 3 whenever: a. A Transmission Operator or Balancing Authority reports one or more cyber attacks on bulk electric system that render an asset(s) unavailable. i. Notification An entity who initiates a Cyber Security Emergency Alert Level 3 shall make notification as per the NERC Functional model or as Regional / local instruction. The Reliability Coordinator shall post the declaration of the alert level along with the location of the affected facility on the RCIS under “CIP” and notify all Transmission Operators and Balancing Authorities in its Reliability Area. The Reliability Coordinator shall also notify the FBI local office, Electricity Sector Information Sharing Analysis Center (ESISAC) and Department of Homeland Security. ii. Updating Status during the Cyber Security Emergency Alert The declaring Entity(ies) shall provide an update of the situation a minimum of once per hour until the Alert Level 3 is terminated. The Reliability Coordinator shall update the RCIS as changes occur. 4. Alert 0 – “Termination of Alert Level” Circumstances: The threat which prompted the Cyber Security Emergency Alert Level has diminished or has been removed. i. Notification An entity who initiates a Cyber Security Emergency Alert shall make notification as per the NERC Functional model or as Regional / local instruction when situation has diminished or returned to normal. The Reliability Coordinator shall notify all other Reliability Coordinators via the RCIS, and it shall also notify all Transmission Operators and Balancing Authorities in its Reliability Area that the Alert Level has been terminated.

Individual

Jimmy Hartmann

ERCOT ISO

Yes

No

The scope should be modified to provide for a different treatment of reporting requirements that are administrative in nature, or that are after-the-fact (thus cannot impact reliability unless analysis and follow-up is not performed; even then, the impact would be at some future time). Reporting requirements which are of the nature to assist in identification of system concerns or which serve to prevent or mitigate on-going system problems (including, but not limited to, actual or attempted sabotage activity) should remain in standards, but should be separate and apart from the administrative reporting.

No

No

The Regional Reliability Organization is not a registered Functional Entity in the NERC registry. The applicability must be revised to more appropriately assign the requirements to registered functional entities. Also, the industry needs to recognize that there are other resources than generation for which the operators need to be included. Perhaps a demand-side resource should have a resource operator. This particular SAR may not be the appropriate venue for this, but control of resources which can be used to mitigate sabotage events or disturbance events may need to be addressed.

Due to the fact that both the CIP-001-1 and EOP-004-1 have similar reporting standards, initially combining the two sounds like a correct analysis. However, after further consideration and due to the critical nature of its intended function involving Security aspects, the CIP-001 should be intensely evaluated to determine if its intended purpose meets the threshold or criteria to stand alone. The existing standards for CIP-001-1 Sabotage Reporting may help prevent future mitigation actions caused by sabotage events. EOP-004-1 Disturbance Reporting is administrative in nature, thus the jeopardy of the Bulk Electric System reliability is

impacted only if analysis is not performed or if corrective follow-up actions are not implemented. Combining EOP-004 Standard requirements under the umbrella of the CIP -001 Standard would create a high profile Disturbance Reporting Standard. The industry would be better served if information defining sabotage was provided as well as a technical reference document on recognizing sabotage that would also clarify or state any personnel training requirements. All aspects of the intended functions must be reviewed before merging the two standards. At a minimum, we must consider modification that provides improved understanding of the reporting standards and implications as they are currently written.

Group

PSEG Enterprise Group Inc Companies

Public Service Electric and Gas Company

Yes

Yes

No

Yes

The PSEG Companies ask that the drafting team allow sufficient flexibility for sabotage recognition and reporting requirements such that nothing precludes utilizing a single corporate-wide program for both bulk electric system assets and other businesses. PSEG's Sabotage Recognition, Response and Reporting Program is directed to all business areas which are directed to follow the same internal protocol that also satisfies the NERC Standards requirements. For example, for gas assets, PSEG's gas distribution business follows the PSEG corporate-wide program for sabotage recognition and response. PSEG agrees that some modifications should be made to CIP-001 (ex. better define or give examples of sabotage) and EOP-004 to make them clearer • If they are merged, then Sabotage will not be in the title (or the primary focus) because several of the Disturbances that reporting is required for in EOP-004 have nothing to do with sabotage. • EOP-004 has criteria listed in 4 places to determine when to send a report: o Criteria listed in EOP-004 Attachment 1 o Criteria listed in EOP-004 Attachment 2 o Criteria listed in top portion of Table 1-EOP-004 o Criteria listed in bottom portion of Table 1-EOP-004 Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable conditions and all of the applicable reports. • If the 2 standards are merged as suggested in the SAR, any differences in the reporting obligation for actual or attempted sabotage and reporting of disturbances must be clear.

Group

Northeast Power Coordinating Council

Northeast Power Coordinating Council

Yes

No

The SAR needs to be more specific in defining its objectives. CIP-001 Requirement R1 currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms "operating personnel" and "sabotage events." The definition of "operating personnel," should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term "sabotage event" needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement

individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be "aware of" such "sabotage events," e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term "aware" in the standard. "Aware" can be interpreted in accordance with its largely passive, dictionary-based meaning, where being "aware" simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of "aware" could refer to more active wording, involving more than mere awareness, e.g., "alert and quick to respond," pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction ...The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ... c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance ..." The sense of Attachment 1 is internally inconsistent between the introduction ("occurs") and the required actions in 6c ("could have resulted in a system disturbance"). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase "or could have resulted in" a potential system disturbance. This inconsistency should be clarified.

No

Yes

Individual

Rick Terrill

Luminant Power

Yes

Yes

Yes

The SAR drafting team should include in the SAR scope a review of the NRC sabotage and event reporting requirements to ensure there are no overlapping or conflicting requirements between NERC, FERC, and the NRC. The SAR scope should include a review of the CIP Cyber Security Standards and coordination with the CIP SDT to ensure that cyber sabotage reporting definitions are in concert, and ensure that cyber sabotage reporting requirements are not duplicated in multiple standards.

Yes

None

Individual

Rao Somayajula

ReliabilityFirst Corporation

Yes

Yes

No

Yes

Individual
Tony Kroskey
Brazos Electric Power Cooperative, Inc.
Yes
Yes
No
No
May need to consider adding Transmission Owner. I don't see a need for the RRO to be included as they are not owner/operators of grid facilities.
Individual
Paul Golden
PacifiCorp
Yes
Yes
No
No
LSE's don't generally own/operate facilities/systems that would experience a logical or physical sabotage event.
Group
Kansas City Power & Light
Kansas City Power & Light
Yes
Agree with the SAR that clarity would be helpful in establishing criteria regarding what constitutes sabotage reporting.
No
Agree with the scope of the SAR except for the applicable entities. See response to question #4.
No
No
Do not agree Load Serving Entities need to continue to be included for sabotage. According the NERC Functional Model, an LSE provides for estimating customer load and provides for the acquisition of transmission and energy to meet customer load demand. An LSE has no real impact on maintaining the reliability of electric network short of their planning function. Unfortunately, an LSE needs to be included for disturbance reporting to the DOE under certain conditions for loss of customer load. This may be a reason to maintain a separation of CIP-001 and EOP-004 so as not to unnecessarily include an LSE when it is not needed.
If it is desirable to keep CIP-001 and EOP-004 separate, it is recommended the SDT consider adding a reference in CIP-001 to the DOE reporting form either by name or by internet link in the standard.

Individual
Terry Harbour
MidAmerican Energy
No
MidAmerican Energy believes only EOP-004-1 is confusing and needs to be modified or clarified. There is no need to combine the two standards. Standard EOP-004 could be clarified to eliminate references to sabotage which are already covered by CIP-001-1. Standard EOP-004 should be strictly limited to system events, not sabotage.
No
See the responses to questions 1 and 5.
Yes
Attachment TOP-005, section 2.9 speaks of "Multi-site sabotage" with no definition. The ES-ISAC 2008 advisory is an associated standard or practice on sabotage. All references to sabotage should be eliminated or retired except for CIP-001.
No
MidAmerican Energy believes the requirement for the Regional Reliability Organization should be removed from EOP-004-1 since the RRO is a holdover from making the standards enforceable. It is no longer appropriate for the regions to be named as responsible entities within the standards.
Conflicting time frames exist from document updates. Reporting should be consolidated to one form and / or site to minimize conflicts, confusion, and errors. 1) Reporting requirements for the outage of 50,000 or more customers in EOP-004-1 requires a report to be made within one hour while the form OE-417 requires a report be made within six hours of the outage. The six hour reference on the updated OE-417 form is the correct reference. 2) Reporting for either CIP-001 or EOP-004 should center on the DOE Form OE-417. This would eliminate confusion, simplify reporting for system operators thereby directly enhancing reliability during system events. This would also eliminate much of the duplicate material and attachments in EOP-004 3) Although it is beyond the scope of this SAR, the industry would benefit if there was a central location or link on the NERC website containing all reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable System Operators to more efficiently locate and report events.
Individual
Darryl Curtis
Oncor Electric Delivery
Yes
Yes
No
Yes
No Additional Comments
Individual
Chris de Graffenried on behalf of Con Edison & O&R
Consolidated Edison Co. of New York, Inc.
Yes
No
GENERAL – CECONY and ORU support the general objectives of the SAR to merge existing standards CIP-001-1 – Sabotage Reporting and EOP-004-1 – Disturbance Reporting to improve clarity and remove redundancy. However, the SAR needs to be more specific in defining its objectives. CIP-001 Requirement R1

currently states: R1. Each Reliability Coordinator, Balancing Authority, Transmission Operator, Generator Operator, and Load Serving Entity shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The SDT needs to include the following objectives: 1. Develop clear definitions for the terms "operating personnel" and "sabotage events." The definition of "operating personnel," should be clarified and limited to staff at BES facilities. Operating personnel should report only those events which meet a clear, recognizable threshold as reportable potential sabotage events. There should be a consistent continent-wide list of examples or typical reportable and non-reportable events to help guide operating personnel. The term "sabotage event" needs to be defined. Clarification is required regarding when the determination of a sabotage event is made, e.g., upon first observation (requiring operating personnel be educated in discerning sabotage events), or upon later investigation by trained security personnel and law enforcement individuals. The terms potential or suspected sabotage event for reporting purposes should be clarified or defined. 2. Define the obligations of Registered Entity operating personnel - who are required to be "aware of" such "sabotage events," e.g., who, what, where, when, why and how, and what they are to do in response to this awareness. The SDT should clarify the use of the term "aware" in the standard. "Aware" can be interpreted in accordance with its largely passive, dictionary-based meaning, where being "aware" simply means knowing about something, such as a sabotage event. Alternatively, the Reliability Standard meaning of "aware" could refer to more active wording, involving more than mere awareness, e.g., "alert and quick to respond," pointing to and requiring a specific affirmative response, i.e., reporting to the appropriate systems, governmental agencies, and regulatory bodies. EOP-004 The SDT needs to work on the following areas. 1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states: Introduction ...The entity on whose system a reportable disturbance occurs shall notify NERC ... 6. Any action taken by a Generator Operator, Transmission Operator, Balancing Authority, or Load-Serving Entity that results in: ... c. Failure, degradation, or misoperation of system protection, special protection schemes, remedial action schemes, or other operating systems that do not require operator intervention, which did result in, or could have resulted in, a system disturbance ..." The sense of Attachment 1 is internally inconsistent between the introduction ("occurs") and the required actions in 6c ("could have resulted in a system disturbance"). The initial intent appears to be only to report actual system disturbances. Yet, paragraph 6c adds the phrase "or could have resulted in" a potential system disturbance. This inconsistency should be clarified.

No

Yes

Individual

Wayne Pourciau

Georgia System Operations Corp.

Yes

There is a need to eliminate burdensome reporting deadlines which interfere with the reliable operations or recovery of the BES. There is also a need to move requirements for reporting to NERC or Regional Entities (except for reporting of threats to physical or cyber security) from the Requirements section of Reliability Standards to elsewhere.

No

The scope of the SAR should be to move all requirements to report to NERC or Regional Entities out of the Requirements section of all Reliability Standards to elsewhere. This does not include reporting, communicating, or coordinating between reliability entities. The NERC/Region reporting requirements could be consolidated in another document and referenced in the Supporting References section of the Reliability Standards. The deadlines for reporting should be changed to realistic timeframes that do not interfere with operating the BES or responding to incidents yet still allow NERC and the Regions to accomplish their missions.

No

Business practices should not be part of a Reliability Standard. Neither should NERC/Region reporting requirements (except for reporting of threats to physical or cyber security). NERC may need to take some action in the case of threats but does not and cannot take any operational action for most of the reporting requirements that are presently in the Requirements section of the Reliability Standards.

No

EOP-004 should be retired. CIP-001 should not apply to LSEs other than those that are retail marketers.

Entity reporting to NERC/Regions is needed by NERC and the Regions to accomplish their missions of overseeing the reliability of the BES and enforcing compliance with Reliability Standards. An entity not reporting as quickly as possible does not harm the integrity of the Interconnection. In fact, it increases the risk to the BES to be investigating details and filling out forms during a time when attention should be on correcting or mitigating an incident.

Individual

Bob Thomas

Illinois Municipal Electric Agency

Yes

Simplification of reporting requirements should facilitate reliability.

Yes

Yes

A one-stop reporting tool/site would facilitate efficient reporting and compliance; e.g., further development of the ES-ISAC/CIPIS to include all reportable categories and automatic notification of required parties. A single report form would be best.

Yes

IMEA recommends the following considerations: Simplification of reportable events and the reporting process should be the overriding objective. NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting (Version 2.0) should be updated to support this standards development initiative. At some point in the process, it may help if examples are given of events actually reported that did not need to be reported.

Individual

Kasia Mihalchuk

Manitoba Hydro

Yes

Yes

No

Yes

Group

IRC Standards Review Committee

IESO

Yes

Yes

No
No
We agree with the applicability of CIP-001-1 but question the need to include the RRO in EOP-004-1. Requirement R1 of EOP-004-1 can be turned into an industry developed and approved procedural requirement with details included in an appendix; whereas R5 can be changed to a requirement for the responsible entities to act on recommendations and to self-report compliance. Tracking and reviewing status of recommendation do not need to be performed by the RRO, or any entity for that matter, if a self-reporting mechanism is developed.
We suggest that the revision not be conducted with a preconceived notion that the two standards must be combined since there are some differences between sabotage and emergency system conditions, and in the communication and reporting processes and channels. We suggest the SDT start off with a neutral position to focus on improving the standards, then assess the pros and cons of merging the two based on technical merit only.
Group
Pepco Holdings, Inc. - Affiliates
Pepco Holdings, Inc.
Yes
PHI recommends merging these two standards into one.
Yes
No
No
As specified in Order 693, Regional Reliability Organizations are not to be assigned applicability. The revised standard(s) should contain the reporting form either directly or by reference and the RRO should be removed. The other EOP-004 requirements for RROs are now considered normal monitoring activities of the Regional Entities.
Consider CIP-008-2 as potentially having overlaps with the proposed standard
Individual
Jim Sorrels
AEP
Yes
No
Sabotage is a term of intent that is often determined after the fact by the registered entity and/or law enforcement officials. In fact, it is often difficult to determine in real-time the intent of a suspicious event. We would suggest that suspicious events become reportable at the point that the event is determined to have had sabotage intent. The entities should have a methodology to collect evidence, to have the evidence analyzed, and to report those events that are determined to have had the intent of sabotage.
Yes
The current reporting process necessitates multiple reports be sent to multiple parties, which is inefficient and may, inadvertently, result in alignment issues between the separate reports. We would recommend that a single report that combines NERC (CIPIS) and NERC ESISAC information be provided to NERC (CIPIS) that is systematically (programmatically) forwarded to all necessary entities. Further, updates to incidents would also go through NERC with the same electronic processing. Currently, we are not aware of a formal method to report incidents to the FBI, which should be also included in the distribution. The current reporting mechanism to the FBI JTTF is by telephone and the NERC platform described would provide more consistent reporting.
No

We would recommend that the Load Serving Entity (LSE) be removed from both standards, and that the Generator Owner and Transmission Owner be added to the resulting standard.
Group
FirstEnergy
FirstEnergy Corp.
Yes
Yes
We agree with the scope but would also like to see the following considered: 1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form. 2. Besides "sabotage", it may be helpful to clearly define "vandalism". It is vaguely written in the standards. Also, the process of "public appeals" for the DOE reportable requirements needs to be more clearly defined. 3. Consolidate documents covering reporting requirements. There are currently several documents that require reporting (EOP-004, CIP-001, DOE oe-417, and NERC's Security Guideline for the Electricity Sector: Threat and Incident Reporting). NERC also has the "Bulk Power System Disturbance Classification Scale" that does not completely align with all the reporting requirements. Therefore we recommend keeping this as simple as possible by combining all the reporting requirements into one standard. It would be beneficial to not require operators to have to go to 4 different documents to determine what to report on.
No
Although we are not aware of any NAESB business practices that need to be reviewed in conjunction with these proposed revisions, the SDT should consider reviewing current RTO procedures and practices that may require the need for variances in the revised standards.
No
The Regional Reliability Organization should be removed from the applicability of EOP-004-1. Any report they receive would be from the other entities listed. For consistency, the entities should report to the appropriate law enforcement agency. A report to the Reliability Entity should also be made for that entities information only.
1. Under Industry Need it states: "The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like." The use of the phrase "more specific" should be qualified by adding "while not being too prescriptive". As with other reliability standards, we do not want a standard that causes unwarranted and unnecessary additional work and costs to an entity to comply. 2. As pointed out by the NERC Audit and Observation Team in the "Issues to be considered" for CIP-001, clarification is needed regarding contacting the FBI. Prior audits dwelled heavily on FBI notification. For example, our policy states that Corporate Security notifies the FBI. In recent events it appears that local law enforcement handles day to day activities. The notification process for contacting the FBI needs clarification along with specific instances in which to call them. Who should make the call to the FBI? It appears that a protocol needs to be developed to clarify what events require notifying the FBI. It could be as simple as after an incident a standard form is completed and forwarded to the FBI, letting them decide if follow up is needed. 3. We suggest aligning all reporting requirements for consistency. The items requiring reporting and the timelines to report are very inconsistent between NERC and the DOE. NERC's timelines are also not consistent with their own Security Guideline for the Electricity Sector: Threat and Incident Reporting.
Individual
Greg Rowland
Duke Energy
Yes
We agree that additional clarity is needed regarding sabotage and disturbance reporting. Requirements should be tightened up and triggering events/thresholds of materiality need to be better defined.
No
While we agree with the need for clarity in sabotage and disturbance reporting, we believe that the Standards Drafting Team should carefully consider whether there is a reliability-related need for each

requirement. Some disturbance reporting requirements are triggered not just to assist in real-time reliability but also to identify lessons-learned opportunities. If disturbance and sabotage reporting continue to be reliability standards, we believe that all linkages to lessons-learned/improvements need to be stripped out. We have other forums to identify lessons-learned opportunities and to follow-up on those opportunities. Also, requirements to report possible non-compliances should be eliminated. We strongly support voluntary self-reporting, but not mandatory self-reporting.

No

No

It's unclear to us that the RRO should continue to be an applicable entity.

Individual

Howard Rulf

We Energies

Yes

No

Consider including the sabotage issues in IRO-014-1 R 1.1.1 footnote 1 and TOP-005-1 Attachment 1, 2.9.

No

Yes

Group

Electric Market Policy

Dominion Resources Inc.

Yes

Comments: Agree with the statement that sabotage is hard to determine in real time by operations staffs. The determination of sabotage should be left up to law enforcement. They have the knowledge and peer contacts needed to adequately determine whether physical or cyber intrusions are merely malicious acts or coordinated efforts (sabotage). The operators should only be required to report physical and cyber intrusions to law enforcement. All other reporting requirements should apply to law enforcement once a determination of sabotage has been made. If the recommendations above are not to be accepted, then we have the following comments: CIP-001-1 1) R1 – states entities “shall have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and “multi-site sabotage” affecting larger portions of the Interconnection. The SAR notes that the industry objects to the multi-site requirement, most likely because the term is ambiguous. If this term remains in the standard, it needs to be clearly defined and responsibilities for obtaining (how do you get this information and from whom?) and distributing need to be included. 2) R1 – audits have shown confusion over the requirement to make operating personnel aware of sabotage events. The term operating personnel needs to be defined. Are they the individuals responsible for operating the facility, coordinating with other entities (i.e., RC, BA, TOP, GOP, and LSE)? It has been suggested that notification is required to all personnel at a facility. Keep in mind the purpose of the standard is to ensure sabotage events are properly reported, not to address emergency response. 3) R1 – The SAR (NERC Audit and Observation Team) notes that Registered Entities have processes and procedures in place, but not all personnel have been trained. There is no specific training requirement in the standard. 4) R2 & R3 – I agree with the SAR that sabotage needs to be defined and these requirements should be more specific with respect to the information to be communicated. It seems to me that the standard should mirror the criteria contained in DOE OE-417. The emphasis should be placed on ensuring that the same information communicated to DOE is shared with the appropriate parties in the Interconnection. 5) R4 – I agree with the SAR (NERC Audit and Observation Team) comments regarding the intention of this requirement. There is no language that directs contact with FBI or RCMP

although that is what is implied by the Purpose statement. 6) VRF Comments – I’m not sure what is intended by the statement “Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.” The purpose of the standard is that of communication. No operational decisions or actions are directed by this standard, nor does it require entities to address operational aspects resulting from sabotage. 7) The potential exists for overlapping sabotage reporting requirements at nuclear power plants due to multiple regulators (Nuclear Regulatory Commission (NRC) – 10 CFR 73 and Federal Energy Regulatory Commission (FERC) – NUC-001-1). Some entities may have revised existing NRC driven procedures to accommodate reporting requirements of both regulators. Because of the restrictions placed on NRC driven documents (i.e., procedures are classified as “safeguards information”), it can be difficult to demonstrate compliance to NERC and/or FERC without ensuring that the individuals are qualified for receipt of such information per 10 CFR 73. Additionally, multiple procedures may have the unintended consequence of delaying appropriate communication. EOP-004-1 Consider removing Attachment 2 as the information is duplicated in DOE Form OE-417. A simple reference to the form should suffice.

Yes

No

No

Applicability should not apply to LSE unless they have physical assets. If they do not have such assets, they are unable to determine how many customers are out, how much load was lost or the duration of an outage. We continue to question the need for the LSE entity in reliability standards. End use customer load is either connected to transmission or distribution facilities. So, the applicable planner has to plan for that load when designing its facilities or the load will not have reliable service. To the extent that energy and capacity for that load is supplied by an entity other than the TO or DP, the TO or DP should have interconnection requirements that compel the supplier to provide any and all data necessary to meet the requirements of reliability standards.

CIP-008-1 Incident Reporting and Response Planning – include some requirements that require coordination with the requirements addressed in this project.

Individual

Jianmei Chai

Consumers Energy Company

Yes

Yes

No

Yes

Individual

Mike Sonnelitter

NextEra Energy Resources, LLC

Yes

No

The scope of the SAR should not include Generator Operators.

No

No
The scope of the proposed SAR should not include the Generator Operator.
No comment.
Individual
D. Bryan Guy
Progress Energy
No
No. It is not clear that the issues listed in a revised standard will improve reliability. Revision based on redundancy is not sufficient reason for combination. Extensive documentation efforts have been made to comply with the current Standards. Unless combining these Standards provides compelling Reliability benefit, it is not worth the industry's resources to revise existing documentation and processes for the sake of eliminating redundancy. Redundancy issues were raised prior to the ERO adopting the initial Standard set into law. We have noted the other issues raised in the SAR, however, it is still unclear where the Reliability benefit of this SAR is evidenced.
No
No. If this SAR moves forward other standards may need to be considered. For example, in CIP-008, incident reporting for cyber incidents leads to filing of the OE-417 form.
Yes
Yes. If this SAR moves forward other practices such as those required by CIP-008 (cyber incident reporting via the OE-417 form) may need to be considered.
Yes
Group
Bonneville Power Administration
BPA Transmission Reliability Program
No
Eliminating a single standard by consolidating two standards does not improve reliability. All of the defined actions are indeed being taken now.
No
Leave as is, all requirements for reporting are now covered. A common definition of sabotage is already widely available.
No
Yes
Individual
Kirit Shah
Ameren
Yes
No
There seems to be an open slate including the following language in the scope "The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards (see tables for each standard at the end of this SAR for more detailed information)." The unnamed improvements should be limited to those requirements that relate only to Disturbance and Sabotage NOT a general wish list(or witch hunt).

No
Yes
None
Group
MRO NERC Standards Review Subcommittee
Michael Brytowski
Yes
No
The MRO NSRS would like to keep the references to the DOE reporting form.
Yes
No
As FERC has directed, the RRO should be removed since they are not owners or operators of the BES.
A. The SAR states that there may be impact on a related standard, COM-003-1 (page SAR-5). Is the SDT referring to Project 2007-02, Operating Personnel Communication Protocols? If so, this is a SAR too and should not be used as a reference. B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard. C. Within EOP-004-1 there is industry confusion on what form to submit in the event of an event. There should only be one form for the new combination Standard eliminating the need for reporting form attachments. It should be the DOE Form, OE-417. Although it is beyond the scope of this SAR, it would greatly benefit industry if there was a central location on the NERC website containing ALL reporting forms, including FERC, NERC, DOE, and ESIAC. This would enable the System Operators to efficiently locate the most current version of the appropriate form in order to report events. D. The word Disturbance is primarily used in other Standards as in, Disturbance Control Standard or system separation due to a disturbance. Should the NERC definition be updated? Should the word "Sabotage" be defined by NERC? Additionally, we recommend that one definition of "Sabotage" be utilized industry-wide, instead of varying definitions by multiple groups like the DOE, ESIAC, etc.