

Standard Authorization Request Form

Title of Proposed Standard: Disturbance and Sabotage reporting (Project 2009-01)
Request Date: April 2, 2009
Approved by SC for posting: April 15, 2009
Revision Date: August 13, 2009

SAR Requester Information	SAR Type <i>(Check a box for each one that applies.)</i>
Name: Patrick Brown	<input type="checkbox"/> New Standard
Primary Contact: Patrick Brown Manager, NERC and Regional Coordination PJM Interconnection	<input checked="" type="checkbox"/> Revision to existing Standard
Telephone: 610-666-4597	<input checked="" type="checkbox"/> Withdrawal of existing Standard
E-mail: brownp@pjm.com	<input type="checkbox"/> Urgent Action

<p>Purpose (Describe the proposed standard action: Nomination of a proposed standard, revision to a standard, or withdrawal of a standard and describe what the standard action will achieve.)</p> <p>This project will entail revision to existing standards CIP-001-1 – Sabotage Reporting and EOP-004-1 – Disturbance Reporting. The standards may be merged to eliminate redundancy and provide clarity on sabotage events. EOP-004 has some ‘fill-in-the-blank’ components to eliminate. The development may include other improvements to the standards deemed appropriate by the drafting team, with the consensus of stakeholders, consistent with establishing high quality, enforceable and technically sufficient bulk power system reliability standards.</p>
<p>Industry Need (Provide a justification for the development or revision of the standard, including an assessment of the reliability and market interface impacts of implementing or not implementing the standard action.)</p> <p>The existing requirements need to be revised to be more specific – and there needs to be more clarity in what sabotage looks like.</p>
<p>Brief Description (Provide a paragraph that describes the scope of this standard action.)</p> <p>CIP-001 may be merged with EOP-004 to eliminate redundancies. Acts of sabotage have to be reported to the DOE as part of EOP-004. Specific references to the DOE form need to be eliminated.</p> <p>EOP-004 has some ‘fill-in-the-blank’ components to eliminate.</p> <p>The development may include other improvements to the standards deemed appropriate by</p>

Standards Authorization Request Form

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).

Detailed Description (Provide a description of the proposed project with sufficient details for the standard drafting team to execute the SAR.)

See "Issues to be Considered by Drafting Team" tables for each standard at the end of this SAR for more detailed information.

Standards Authorization Request Form

Reliability Functions

The Standard will Apply to the Following Functions <i>(Check box for each one that applies.)</i>		
<input checked="" type="checkbox"/>	Reliability Coordinator	Responsible for the real-time operating reliability of its Reliability Coordinator Area in coordination with its neighboring Reliability Coordinator's wide area view.
<input checked="" type="checkbox"/>	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within a Balancing Authority Area and supports Interconnection frequency in real time.
<input type="checkbox"/>	Interchange Authority	Ensures communication of interchange transactions for reliability evaluation purposes and coordinates implementation of valid and balanced interchange schedules between Balancing Authority Areas.
<input type="checkbox"/>	Planning Coordinator	Assesses the longer-term reliability of its Planning Coordinator Area.
<input type="checkbox"/>	Resource Planner	Develops a >one year plan for the resource adequacy of its specific loads within a Planning Coordinator area.
<input type="checkbox"/>	Transmission Planner	Develops a >one year plan for the reliability of the interconnected Bulk Electric System within its portion of the Planning Coordinator area.
<input type="checkbox"/>	Transmission Service Provider	Administers the transmission tariff and provides transmission services under applicable transmission service agreements (e.g., the pro forma tariff).
<input checked="" type="checkbox"/>	Transmission Owner	Owns and maintains transmission facilities.
<input checked="" type="checkbox"/>	Transmission Operator	Ensures the real-time operating reliability of the transmission assets within a Transmission Operator Area.
<input checked="" type="checkbox"/>	Distribution Provider	Delivers electrical energy to the End-use customer.
<input checked="" type="checkbox"/>	Generator Owner	Owns and maintains generation facilities.
<input checked="" type="checkbox"/>	Generator Operator	Operates generation unit(s) to provide real and reactive power.
<input type="checkbox"/>	Purchasing-Selling Entity	Purchases or sells energy, capacity, and necessary reliability-related services as required.
<input type="checkbox"/>	Market Operator	Interface point for reliability functions with commercial functions.
<input checked="" type="checkbox"/>	Load-Serving Entity	Secures energy and transmission service (and reliability-related services) to serve the End-use Customer.

Standards Authorization Request Form

Reliability and Market Interface Principles

Applicable Reliability Principles <i>(Check box for all that apply.)</i>	
<input checked="" type="checkbox"/>	1. Interconnected bulk power systems shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
<input type="checkbox"/>	2. The frequency and voltage of interconnected bulk power systems shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
<input checked="" type="checkbox"/>	3. Information necessary for the planning and operation of interconnected bulk power systems shall be made available to those entities responsible for planning and operating the systems reliably.
<input checked="" type="checkbox"/>	4. Plans for emergency operation and system restoration of interconnected bulk power systems shall be developed, coordinated, maintained and implemented.
<input type="checkbox"/>	5. Facilities for communication, monitoring and control shall be provided, used and maintained for the reliability of interconnected bulk power systems.
<input type="checkbox"/>	6. Personnel responsible for planning and operating interconnected bulk power systems shall be trained, qualified, and have the responsibility and authority to implement actions.
<input type="checkbox"/>	7. The security of the interconnected bulk power systems shall be assessed, monitored and maintained on a wide area basis.
<input checked="" type="checkbox"/>	8. Bulk power systems shall be protected from malicious physical or cyber attacks.
Does the proposed Standard comply with all of the following Market Interface Principles? <i>(Select 'yes' or 'no' from the drop-down box.)</i>	
1. A reliability standard shall not give any market participant an unfair competitive advantage. Yes	
2. A reliability standard shall neither mandate nor prohibit any specific market structure. Yes	
3. A reliability standard shall not preclude market solutions to achieving compliance with that standard. Yes	
4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards. Yes	

Standards Authorization Request Form

Related Standards

Standard No.	Explanation
COM-003-1	Operations Communications Protocols – this standard may include some requirements that require coordination with the requirements addressed in this project. (still in standard development stage)
IRO-014-1	R1.1.1, footnote 1 lists sabotage. The standard drafting team should consider this reference and the impact of their work on this specific item.
TOP-005-1.1	Attachment 1, item 2.9 is “Multi-site sabotage”. The standard drafting team should consider this reference and the impact of their work on this specific item.

Related SARs

SAR ID	Explanation

Regional Variances

Region	Explanation
ERCOT	
FRCC	
MRO	
NPCC	
SERC	
RFC	
SPP	
WECC	

Issues to be Considered by Drafting Team Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	Title
CIP-001-0	Sabotage Reporting
Issues	<p>FERC Order 693</p> <p>Disposition: Approved with modifications</p> <ul style="list-style-type: none"> • Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. • Define “sabotage” and provide guidance on triggering events that would cause an entity to report an event. • In the interim, provide advice to entities about the reporting of particular circumstances as they arise. • Consider FirstEnergy’s suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. • Incorporate a periodic review or updating of the sabotage reporting procedures and for their periodic testing. Consider a staggered schedule of annual testing and formal review every two to three years. • Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. • Explore ways to reduce redundant reporting, including central coordination of sabotage reports and a uniform reporting format. <p>V0 Industry Comments</p> <ul style="list-style-type: none"> • Object to multi-site requirement • Definition of sabotage required <p>VRF comments</p> <ul style="list-style-type: none"> • Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures. <p>Other</p> <ul style="list-style-type: none"> • Modify standard to conform to the latest version of NERC’s Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure. <p>NERC Audit and Observation Team</p> <ul style="list-style-type: none"> • Applicability — How does this standard pertain to Load Serving Entities, LSE's. • Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained. • Question: How do you “and make the operator aware” • R4 — “What is meant by: “establish contact with the FBI”. Is a phone number adequate? Many entities which call the FBI are referred back to the local authority. The AOT noted that on the FBI website it states

	<p>to contact the local authorities. Is this a question for Homeland Security to deal with for us?"</p> <ul style="list-style-type: none"> R4 — Establish communications contacts, as applicable with local FBI and RAMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? <p>FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000</p> <ul style="list-style-type: none"> In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: <ul style="list-style-type: none"> FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf) NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf), FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.
--	---

Issues to be Considered by Drafting Team	
Project 2009-01 — Disturbance and Sabotage Reporting	
Standard #	Title
EOP-004-1	Disturbance Reporting
Issues	<p>FERC Order 693</p> <p>Disposition: Approved with modification</p> <ul style="list-style-type: none"> Include any requirements for users, owners, and operators of the bulk power system to provide data that will assist NERC in the investigation of a blackout or disturbance. Change NERC's Rules of Procedure to assure the Commission receives these reports in the same frame as the DOE. Consider APPA's concern about generator operators and LSEs analyzing performance of their equipment and provide data and information on the equipment to assist others with analysis. Consider all comments offered in a future modification of the reliability standard.

	<p>Fill-in-the-Blank Team Comments</p> <ul style="list-style-type: none">• Consider changes to R1 and R3.4 to standardize the disturbance reporting requirements (requirements for disturbance reporting need to be added to this standard)• Regions currently have procedures, but not in the form of a standard. The drafting team will need to review regional requirements to determine reporting requirements for the North American standard. <p>V0 Industry Comments</p> <ul style="list-style-type: none">• R3 – too many reports, narrow requirement to RC• How does this apply to generator operator? <p>Other</p> <ul style="list-style-type: none">• Modify standard to conform to the latest version of NERC's Reliability Standards Development Procedure, the NERC Standard Drafting Team Guidelines, and the ERO Rules of Procedure. <p>NERC Audit and Observation Team</p> <ul style="list-style-type: none">• R3.1 — Can there be a violation without an event? <p>Event Analysis Team</p> <ul style="list-style-type: none">• Reliability Issue: Coordination and follow up on lessons learned from event analyses Consider adding to EOP-004 – Disturbance Reporting. Proposed requirement: Regional Entities (REs) shall work together with Reliability Coordinators, Transmission Owners, and Generation Owners to develop an Event Analysis Process to prevent similar events from happening and follow up with the recommendations. This process shall be defined within the appropriate NERC Standard. <p>FERC's December 20, 2007 and April 4, 2008 Orders in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000</p> <ul style="list-style-type: none">• In FERC's December 20, 2007 Order, the Commission reversed NERC's Compliance Registry decisions with respect to three load serving entities in the ReliabilityFirst (RFC) footprint. The distinguishing feature of these three LSEs is that none owned physical assets. Both NERC and RFC assert that there will be a "reliability gap" if retail marketers are not registered as LSEs. To avoid a possible gap, a consistent, uniform approach to ensure that appropriate Reliability Standards and associated requirements are applied to retail marketers must be applied. Each drafting team responsible for reliability standards applicable to LSEs is to review and change as necessary, requirements in the applicable reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see:<ul style="list-style-type: none">• FERC's December 20, 2007 Order (http://www.nerc.com/files/LSE_decision_order.pdf)• NERC's March 4, 2008 (http://www.nerc.com/files/FinalFiledLSE3408.pdf),• FERC's April 4, 2008 Order (http://www.nerc.com/files/AcceptLSECompFiling-040408.pdf) and• NERC's July 31, 2008 (http://www.nerc.com/files/FinalFiled-CompFiling-LSE-07312008.pdf) compliance filings to FERC on this subject.
--	--

Comments received on Project 2009-01 — Disturbance and Sabotage Reporting

The Disturbance and Sabotage Reporting Standard Drafting Team (DSR SDT) received many suggestions for improvements to the standards during the SAR comment period. These comments do not indicate any revisions to the SAR, but the DSRSDT thought that these comments merited further consideration during the standard drafting phase of the project. The comments below are being compiled for use by the Standard Development Team.

Organization	Comment
Electric Market Policy	<p>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:</p> <p>CIP-001-1</p> <ol style="list-style-type: none"> 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.

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	<p>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.</p> <p>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-004-1Consider removing Attachment 2 as the information is duplicated in DOE Form OE-417. A simple reference to the form should suffice.</p>
Lands Energy Consulting	<p>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.</p> <p>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.</p> <p>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.</p>
Calpine Corporation	Communication of facility status or emergencies between merchant generators registered as GOP and the RC, BA,

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	<p>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.</p>
Covanta	<p>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.</p>
Northeast Power Coordinating Council	<p>The SAR needs to be more specific in defining its objectives.</p> <p>CIP-001 Requirement R1 currently states:</p> <p>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.</p> <p>The SDT needs to include the following objectives:</p> <ol style="list-style-type: none"> 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.

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	<p>EOP-004 - The SDT needs to work on the following areas.</p> <p>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.</p>
FirstEnergy	<p>We agree with the scope but would also like to see the following considered:</p> <p>1. References to the DOE reporting process in EOP-004 need to be revised. They currently refer to the old EIA form.</p> <p>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.</p> <p>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.</p>
MRO NERC Standards Review Subcommittee	<p>The MRO NSRS would like to keep the references to the DOE reporting form.</p>
Cowlitz County PUD	<p>Added to the scope:</p> <p>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.</p> <p>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.</p>
Reliant Energy	<p>I think Generator operators should be excluded except to provide requested information from the System Operator or</p>

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	Reliability coordinator.
ERCOT ISO	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.
Consolidated Edison Co. of New York, Inc.	<p>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.</p> <p>However, the SAR needs to be more specific in defining its objectives.</p> <p>CIP-001 Requirement R1 currently states:</p> <p>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.</p> <p>The SDT needs to include the following objectives:</p> <ol style="list-style-type: none"> 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. <p>EOP-004 - The SDT needs to work on the following areas.</p>

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	<p>1. NERC reporting needs to be clarified. For example, Attachment 1 paragraph 6c states:</p> <p>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.</p> <p>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.</p>
Georgia System Operations Corp.	<p>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.</p>
AEP	<p>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.</p>
Duke Energy	<p>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.</p>
NextEra Energy Resources, LLC	<p>The scope of the SAR should not include Generator Operators.</p>

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
Luminant Power	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.
Illinois Municipal Electric Agency	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.
AEP	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.
Kansas City Power & Light	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.
Electric Market Policy	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.
Lands Energy Consulting	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'

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	<p>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.</p>
<p>Calpine Corporation</p>	<p>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.</p>
<p>Covanta</p>	<p>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.</p>
<p>Reliant Energy</p>	<p>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.</p>
<p>Texas Regional Entity</p>	<p>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</p>

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	(TO) should also be added to the list of applicability for reporting sabotage on its facilities.
Exelon	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..."
ERCOT ISO	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.
AEP	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.
NextEra Energy Resources, LLC	The scope of the proposed SAR should not include the Generator Operator.
PSEG Enterprise Group Inc Companies	<p>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:</p> <ul style="list-style-type: none"> 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 <p>Therefore, it would be much easier if there was one table of criteria for reference that addressed all of the reportable</p>

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	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.
FirstEnergy	<p>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.</p> <p>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.</p>
MRO NERC Standards Review Subcommittee	<p>B. CIP-001-1 and EOP-004-1 should be combined into one EOP Standard.</p> <p>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.</p>
Lands Energy Consulting	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.
Colmac Clarion	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.
Cowlitz County PUD	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

Consideration of Comments on Project 2009-01 — SAR for Disturbance and Sabotage Reporting

Organization	Comment
	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.
ERCOT ISO	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.
MidAmerican Energy	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 and 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.
Illinois Municipal Electric Agency	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.