NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Project 2009-01 Disturbance and Sabotage Reporting Consideration of Issues and Directives

Project 2009-01 Disturbance and Sabotage Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
"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 to contact the local authorities. Is this a question for Homeland Security to deal with for us?" Establish communications contacts, as applicable with local FBI and RCMP officials. Some entities are very remote and the sheriff is the only local authority does the FBI still need to be contacted? Registered Entities have sabotage reporting processes and procedures in place but not all personnel has been trained.	CIP-001-1 NERC Audit Observation Team	The DSR SDT has been in contact with FBI staff and developed a notification flow chart for law enforcement as it pertains to EOP-004. The “Background” section of the standard outlines the reporting hierarchy that exists between local, state, provincial and federal law enforcement. The entity experiencing an event should notify the appropriate state or provincial law enforcement agency that will then coordinate with local law enforcement for investigation. These local, state and provincial agencies will coordinate with higher levels of law enforcement or other governmental agencies.

Question: How do you “and make the operator aware”	CIP-001-1 NERC Audit Observation Team	This has been removed from the standard. Requirement R1, Part 1.1 requires that the entity has a process for recognizing events.
How does this standard pertain to Load Serving Entities, LSE's.	CIP-001-1 NERC Audit Observation Team	LSE is an applicable entity since LSEs are currently applicable under CIP-008.
We direct the ERO to explore ways to address these concerns – including central coordination of sabotage reports and a uniform reporting format – in developing modifications to the Reliability Standard with the appropriate governmental agencies that have levied the reporting requirements.	CIP-001-1; Order 693	See “Background” section of the standard.

"Define “sabotage” and provide guidance on triggering events that would cause an entity to report an event. Paragraph 461. Several commenters agree with the Commission’s concern that the term “sabotage” should be defined. For the reasons stated in the NOPR, we direct that the ERO further define the term and provide guidance on triggering events that would cause an entity to report an event. However, we disagree with those commenters that suggest the term “sabotage” is so vague as to justify a delay in approval or the application of monetary penalties. As explained in the NOPR, we believe that the term sabotage is commonly understood and that common understanding should suffice in most instances.	CIP-001-1; Order 693	The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of “event”. The DSR SDT considered the FERC directive to “further define sabotage” and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term “sabotage” is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

The ERO should consider suggestions raised by commenters such as FirstEnergy and Xcel to define the specified period for reporting an incident beginning from when an event is discovered or suspected to be sabotage, and APPA's concerns regarding events at unstaffed or remote facilities, and triggering events occurring outside staffed hours at small entities.	CIP-001-1; Order 693	Attachment 1 defines the timelines and events which are to be reported under this standard. The required reporting is either one hour or 24 hours (depending on the type of event) "of recognition of the event."

Modify CIP-001-1 1 to require an applicable entity to contact appropriate governmental authorities in the event of sabotage within a specific period of time, even if it is a preliminary report. Further, in the interim while the matter is being addressed by the Reliability Standards development process, we direct the ERO to provide advice to entities that have concerns about the reporting of particular circumstances as they arise.	CIP-001-1; Order 693	Per Requirement R1, the entity is to develop procedure(s) that include event reporting to law enforcement and governmental agencies. The DSR SDT also proposes revisions to the NERC Rules of Procedure to report events to the FERC. 812. NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.

Consider the need for wider application of the standard. Consider whether separate, less burdensome requirements for smaller entities may be appropriate. Paragraph 458. The Commission acknowledges the concerns of the commenters about the applicability of CIP-001-1 to small entities and has addressed the concerns of small entities generally earlier in this Final Rule. Our approval of the ERO Compliance Registry criteria to determine which users, owners and operators are responsible for compliance addresses the concerns of APPA and others. 459. However, the Commission believes that there are specific reasons for applying this Reliability Standard to such entities, as discussed in the NOPR. APPA indicates that some small LSEs do not own or operate "hard assets" that are normally thought of as "at risk" to sabotage. The Commission is concerned that, an adversary might determine that a small LSE is the appropriate target when the adversary aims at a particular population or facility. Or an adversary may target a small user, owner or operator because it may have similar equipment or protections as a larger facility, that is, the adversary may use an attack against a smaller facility as a training "exercise." {continued below}	CIP-001-1; Order 693	Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

The knowledge of sabotage events that occur at any facility (including small facilities) may be helpful to those facilities that are traditionally considered to be the primary targets of adversaries as well as to all members of the electric sector, the law enforcement community and other critical infrastructures. 460. For these reasons, the Commission remains concerned that a wider application of CIP-001-1 may be appropriate for Bulk Power System reliability. Balancing these concerns with our earlier discussion of the applicability of Reliability Standards to smaller entities, we will not direct the ERO to make any specific modification to CIP-001-1 to address applicability. However, we direct the ERO, as part of its Work Plan, to consider in the Reliability Standards development process, possible revisions to CIP-001-1 that address our concerns. Regarding the need for wider application of the Reliability Standard. Further, when addressing such applicability issues, the ERO should consider whether separate, less burdensome requirements for smaller entities may be appropriate to address these concerns.		

The Commission affirms the NOPR directive and directs the ERO to incorporate a periodic review or updating of the sabotage reporting procedures and for the periodic testing of the sabotage reporting procedures. At this time, the commission does not specify a review period as suggested by FirstEnergy and MRO and, rather, believes that the appropriate period should be determined through the ERO's Reliability Standards development process. However, the Commission directs that the ERO begin this process by considering a staggered schedule of annual testing of the procedures with modifications made when warranted formal review of the procedures every two or three years.	CIP-001-1; Order 693	The standard is responsive this directive with the following language in Requirement R3: R3. Each Responsible Entity shall conduct an annual test, not including notification to the Electric Reliability Organization, of the communications process in Part 1.2. The DSR SDT envisions that this will include verification that contact information contained in the Operating Plan is correct. As an example, the annual update of the Operating Plan could include calling others as defined in the Responsibility Entity's Operating Plan (see Part 1.2) to verify that their contact information is correct and current. If any discrepancies are noted, the Operating Plan would be updated.

Consider FirstEnergy's suggestions to differentiate between cyber and physical security sabotage and develop a threshold of materiality. Paragraph 451. A number of commenters agree with the Commission's concern that the term sabotage" needs to be better defined and guidance provided on the triggering events that would cause an entity to report an event. FirstEnergy states that this definition should differentiate between cyber and physical sabotage and should exclude unintentional operator error. It advocates a threshold of materiality to exclude acts that do not threaten to reduce the ability to provide service or compromise safety and security. SoCal Edison states that clarification regarding the meaning of sabotage and the triggering event for reporting would be helpful and prevent over reporting.	CIP-001-1; Order 693	This addressed in Attachment 1. There are specific event types for both cyber and physical security with their respective report submittal requirements.

"Include a requirement to report a sabotage event to the proper government authorities. Develop the language to specifically implement this directive. Paragraph 467. CIP-001-1, Requirement R4, requires that each applicable entity establish communications contacts, as applicable, with the local FBI or Royal Canadian Mounted Police officials and develop reporting procedures as appropriate to its circumstances. The Commission in the NOPR expressed concern that the Reliability Standard does not require an applicable entity to actually contact the appropriate governmental or regulatory body in the event of sabotage. Therefore, the Commission proposed that NERC modify the Reliability Standard to require an applicable entity to "contact appropriate federal authorities, such as the Department of Homeland Security, in the event of sabotage within a specified period of time."212 468. As mentioned above, NERC and others object to the wording of the proposed directive as overly prescriptive and note that the reference to "appropriate federal authorities" fails to recognize the international application of the Reliability Standard. The example of the Department of Homeland Security as an "appropriate federal authority" was not intended to be an exclusive designation. Nonetheless, the Commission agrees that a reference to "federal authorities" could create confusion. Accordingly, we modify the direction in the NOPR and now direct the ERO to address our underlying concern regarding mandatory reporting of a sabotage event. The ERO's Reliability Standards development process should develop the language to implement this directive."		See Background section of Standard. A proposal discussed with FBI, FERC Staff, NERC Standards Project Coordinator and SDT Chair is reflected in the flowchart below (Reporting Hierarchy for Event EOP-004-2). Essentially, reporting an event to law enforcement agencies will only require the industry to notify the state or provincial level law enforcement agency. The state or provincial level law enforcement agency will coordinate with local law enforcement to investigate. If the state or provincial level law enforcement agency decides federal agency law enforcement or the RCMP should respond and investigate, the state or provincial level law enforcement agency will notify and coordinate with the FBI or the RCMP.

On March 4, 2008, NERC submitted a compliance filing in response to a December 20, 2007 Order, in which the Commission reversed a NERC decision to register three retail power marketers to comply with Reliability Standards applicable to load serving entities (LSEs) and directed NERC to submit a plan describing how it would address a possible "reliability gap" that NERC asserted would result if the LSEs were not registered. NERC's compliance filing included the following proposal for a short-term plan and a long-term plan to address the potential gap: · Short-term: Using a posting and open comment process, NERC will revise the registration criteria to define "Non-Asset Owning LSEs" as a subset of Load Serving Entities and will specify the reliability standards applicable to that subset. · Longer-term: NERC will determine the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers and process them through execution of the three-year Reliability Standards Development Plan. In this revised Reliability Standards Development Plan, NERC is commencing the implementation of its stated long-term plan to address the issues surrounding accountability for loads served by retail marketers/suppliers. The NERC Reliability Standards Development Procedure will be used to identify the changes necessary to terms and requirements in reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. Specifically, the following description has been incorporated into the scope for	CIP-001-1 and EOP-004 ORDER ON ELECTRIC RELIABILITY ORGANIZATION REGISTRY_DETERMINATIONS; ORDER ON COMPLIANCE FILING	The LSE is an applicable entity, since LSEs are currently applicable under CIP-008. If an entity owns distribution assets, that entity will be registered as a Distribution Provider. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.

affected projects in this revised Reliability Standards Development Plan that includes a standard applicable to Load Serving Entities: Source: FERC's December 20, 2007 Order in Docket Nos. RC07-004-000, RC07-6-000, and RC07-7-000. Issue: 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 own 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 followed. Each drafting team responsible for reliability standards that are applicable to LSEs is to review and change as necessary, requirements in the reliability standards to address the issues surrounding accountability for loads served by retail marketers/suppliers. For additional information see: · 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.		

Object to multi-site requirement	Version 0 Team CIP-001-1	The Standard was revised for clarity. Attachment 1 defines the timelines and events which are to be reported under this standard. The applicable entities are also identified for each type of event.
Definition of sabotage required VRFs Team Adequate procedures will insure it is unlikely to lead to bulk electric system instability, separation, or cascading failures.	Version 0 Team CIP-001-1	No definition for sabotage was developed The DSR SDT has not proposed a definition for inclusion in the NERC Glossary because it is impractical to define every event that should be reported without listing them in the definition. Attachment 1 is the de facto definition of "event". The DSR SDT considered the FERC directive to "further define sabotage" and decided to eliminate the term sabotage from the standard. The team felt that without the intervention of law enforcement after the fact, it was almost impossible to determine if an act or event was that of sabotage or merely vandalism. The term "sabotage" is no longer included in the standard and therefore it is inappropriate to attempt to define it. The events listed in Attachment 1 provide guidance for reporting both actual events as well as events which may have an impact on the Bulk Electric System. The DSR SDT believes that this is an equally effective and efficient means of addressing the FERC Directive.

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	Events Analysis Team Reliability Issue	The DSR SDT envisions EOP-004-2 to be a reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
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.	Fill in the Blank Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.
Can there be a violation without an event?	NERC Audit Observation Team	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. In the opinion of the DSR SDT, there cannot be a violation of Requirement R2 without an event. Since Requirement R1 calls for an Operating Plan, there can be a violation of R1 without an event.

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. Paragraph 607. APPA is concerned about the scope of Requirement R2 because, in its opinion, Requirement R2 appears to impose an open-ended obligation on entities such as generation operators and LSEs that may have neither the data nor the tools to promptly analyze disturbances that could have originated elsewhere. APPA proposes that Requirement R2 be modified to require affected entities to promptly begin analyses to ensure timely reporting to NERC and DOE.	EOP-004-1 Order 693	The DSR SDT envisions EOP-004-2 to be a continent-wide reporting standard. Any follow up investigation or analysis falls under the purview of the NERC Events Analysis Program under the NERC Rules of Procedure.

From: David Cook Sent: Wednesday, July 16, 2008 6:06 PM To: Rick Sergel; Dave Nevius; David A. Whiteley; Management Subject: RE: FERC request for DOE-417s I agree the real fix is to revise the EOP-004 standard. I agree that we can't (and shouldn't try) to do that by way of amendments to our Rules of Procedure. So we should include that fix in the standards work plan, do the best we can in the meantime to provide FERC with the 417s, and I'll have the conversation with Joe McClelland about not being able to do what the Commission directed in Order 693 (i.e., change the standards by way of a change in the Rules of Procedure). David	EOP-004-1 Other	Per Requirement R1, the entity is to develop procedure(s) that include event reporting to law enforcement and governmental agencies. The DSR SDT also proposes revisions to the NERC Rules of Procedure to report events to the FERC. 812. NERC will establish a system to collect report forms as established for this section or standard, from any Registered Entities, pertaining to data requirements identified in Section 800 of this Procedure. Upon receipt of the submitted report, the system shall then forward the report to the appropriate NERC departments, applicable regional entities, other designated registered entities, and to appropriate governmental, law enforcement, regulatory agencies as necessary. This can include state, federal, and provincial organizations.

In response to a SAR submitted by Glenn Kaht of ReliabilityFirst: As part of a regional compliance violation investigation, a possible reliability gap was identified related to EOP-004-1 — Disturbance Reporting. The existing standard limits reporting of generation outages to just those outages associated with loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. This requirement has been interpreted as meaning that only generation outages that must be reported are those that occur with the loss of a bulk power transmission element. By not reporting large generation losses that occur without the loss of a bulk power transmission element, the industry is overlooking a potential opportunity to identify and learn from these losses. Specifically, Item 1 of Attachment 1 of EOP-004 requires the reporting of events if "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations. Generally, a disturbance report will be required if the event results in actions such as:" The Standard then lists six different actions that may occur as a result of the event in order to be reportable. All six of these actions appear to be dependent on "The loss of a bulk power transmission component that significantly affects the integrity of interconnected system operations" in order for the event to be reportable. Some of these events may significantly impact the reliable operation of the bulk power system. Consider a revision to EOP-004-1 — Disturbance Reporting requiring a Generator Operator (GOP) that	Standards Committee Action From 01/13/2010	The DSR SDT has worked closely with the NERC EAWG to develop the event reporting requirements shown in Attachment 1. The EAWG and the DSR SDT considered this request and weighed it against reliability needs for reporting.

experiences the loss of generation greater than 500 MW that results in modification of equipment (e.g. control systems, or Power Load Unbalancer (PLU)) to be a reportable event.		
too many reports, narrow requirement to RC	Version 0 Team	There is only one report required under this standard. An entity may submit the report using Attachment 2 or the DEO OE-417 report form.
How does this apply to generator operator?	Version 0 Team	See attachment 1 for specific generator operator applicability.