



AESO Reliability Committee (ARC) Security Work Group (SWG) Standard Review Meeting

ARC Security Work Group

Chair: Garry Spicer

Alternate Chairs: Doug Hincks, Jack Kelly

The AESO Reliability Committee (ARC) Security Work Group (SWG) is responsible for reviewing the North American Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) reliability standards to assess applicability of the standard requirements within Alberta. The group will also be examining measures and entity responsibilities for these standards. These activities are carried out in accordance with the ARC SWG Terms of Reference (DRAFT).

Summary of Previous Meeting

Date of meeting: Thursday, 09 October, 2008, 9am – Noon.

Location: Enmax

Outcomes:

- The SWG welcomed several new members
- The SWG reviewed the outcomes of the previous meeting (17 September).
- The SWG discussed the current status of the CIP standards review by NERC. Specifically, the CIP-002 through CIP-009 standards are being revised.
- The SWG discussed the current status of proposed legislative changes in the U.S. that would affect FERC authority in relation to the CIP standards. It appears that this legislation has been deferred and won't be passed before the U.S. election.
- The SWG received the following briefings:
 - Ken Gardner presented additional detail regarding the Alberta Reliability Standards process by which standards, such as the CIPs, will be implemented within the province
 - Garry Spicer presented the current approach for the SWG. This is to focus current efforts on the CIP-001 standard (Sabotage Reporting), since it is the only CIP standard that is currently stable. Definitions and requirements will be reviewed first. Measures and other aspects of the standard will then be reviewed.
- The SWG enumerated which of its members still needed binders for workgroup activities. Binders will be sent to those members who indicated a need.

- The SWG discussed potential dates for future meetings. It was decided to hold a second meeting in November, rather than attempt to meet during December. (See section below regarding upcoming meetings)
-
- The SWG members discussed a number of questions and concerns regarding the NERC CIP-001 requirements. A brief summary of these includes:
 - What are the reporting thresholds?
 - How to distinguish sabotage from vandalism and theft
 - How to determine intent or perceived intent
 - How to assess the potential affect on grid reliability
 - How far to go when “erring on the side of caution”
 - Sabotage may have different degrees of relevance to different entity types.
 - Does the standard apply to both physical and cyber sabotage?
 - Are there potential overlaps with CIP-008? Incidents and sabotage may overlap if an incident is caused by a deliberate act.
 - There are different types of sabotage. Some events are critical and require prompt response. Others are less time critical but may be part of a longer term pattern.
 - What processes are needed to stand down from an alert status after a report of sabotage, attempted sabotage, or a sabotage threat?
 - Clarity is important with regards to confirmation of compliance with sabotage reporting standards.
 - Are there requirements for specific information to be provided in a sabotage report?
 - The requirement to establish communication contacts and reporting procedures with police / government authorities has proven difficult in some U. S. jurisdictions, due to challenges identifying participants from the relevant police services and government authorities.
 - Some of the existing CIP requirements seem to embed more than one actual requirement. How will entities be assessed in such situations?
 - Due to local, provincial, and federal jurisdiction issues, how will the standards address reporting to local police services and provincial services, such as ASSIST?
 - Will these standards address the flow of information from authorities, such as police and security intelligence services? How will information be shared amongst AIES entities?
- The SWG reviewed a draft definition for “Sabotage”. This definition will help to shape sabotage reporting standards in Alberta.
 - EPCOR provided a copy of its current sabotage reporting procedures, which contains a definition for sabotage.
 - Various edits were suggested for the draft definition based on the input noted above. The group felt that these would simplify and clarify the definition.

- A question was raised about whether market systems would be included in the scope of sabotage reporting. It was agreed that this matter would be referred to the ARC for clarification.
- Discussion was held about the difference between time critical sabotage (events that need to be promptly reported to the AESO System Controller as well as to police / government authorities for urgent response) and less time critical sabotage (events that need to be reported to police / government authorities for follow up / analysis). Entities may be in the best position to assess this if provided with appropriate guidance.
- The group generally agreed that sabotage referred to both physical and cyber sabotage, to the extent that these can affect the reliability of the AIES.

Schedule for Upcoming Security Work Group Meetings

Meeting Date	Location
Thursday, 06 November 2008 (9:00 am to 12:00 pm)	Enmax
Thursday, 27 November 2008 (9:00 am to 12:00 pm) (<i>Tentative</i>)	Enmax

Upcoming Meeting Agenda (06 November 2008)

1. Review outcomes from the previous meeting.
2. Discuss the definition of Sabotage, with revisions based on the last meeting.
3. As time permits, review a draft Alberta reliability standard, as prepared by the AESO, based on the following NERC reliability standard:
 - CIP-001-1 – Sabotage Reporting:
 - <http://www.nerc.com/files/CIP-001-1.pdf>

Please bring paper copies of the standard(s) to be reviewed to the meetings. If you have material (e.g. existing documented practices or procedures) that you believe would be helpful to the SWG, and you are willing to share the material with the SWG members, then please bring copies to the meetings.

If you are planning to attend the next Security Work Group meeting, then please RSVP to allison.mathews@aeso.ca one week prior to the meeting.