



## **AESO Reliability Committee (ARC) Security Work Group (SWG) Kickoff Meeting**

---

The ARC Security Work Group is responsible for reviewing the NERC Critical Infrastructure Protection reliability standards to assess applicability of the standard requirements within Alberta. The group will also be examining measures and entity responsibilities for these standards.

### **ARC Security Work Group Meeting**

Chair: Garry Spicer

Alternate Chairs: Doug Hincks, Jack Kelly

Date of first meeting: Wednesday, 17 September, 2008, 9am – Noon.

Location: AESO Office, 2500, 330 5<sup>th</sup> Avenue SW

### **Agenda:**

#### Welcome and Introductions

- Purpose and objectives for the SWG
- Determine potential dates for future meetings

#### Background

- Review ARC Standard Review Process
- Review ARC Security Work Group Terms of Reference (Draft)
- Review ARC Reliability Standards Review Template

#### Review approach for assessing CIP standards

- Review the NERC reliability standard format
- Discuss applicability of standards to different entity types and sizes

Determine which NERC Critical Infrastructure Protection (CIP) standards to assess at future meetings. The standards include:

- CIP-001-1 – Sabotage Reporting:
  - <http://www.nerc.com/files/CIP-001-1.pdf>
- CIP-002-1 – Cyber Security – Critical Cyber Asset Identification:
  - <http://www.nerc.com/files/CIP-002-1.pdf>
- CIP-003-1 – Cyber Security – Security Management Controls:
  - <http://www.nerc.com/files/CIP-003-1.pdf>

- CIP-004-1 – Cyber Security – Personnel and Training:
  - <http://www.nerc.com/files/CIP-004-1.pdf>
- CIP-005-1 – Cyber Security – Electronic Security Perimeter:
  - <http://www.nerc.com/files/CIP-005-1.pdf>
- CIP-006-1 – Cyber Security – Physical Security:
  - <http://www.nerc.com/files/CIP-006-1.pdf>
- CIP-006-1 a– Cyber Security – Physical Security:
  - <http://www.nerc.com/files/CIP-006-1a.pdf>
- CIP-007-1 – Cyber Security – Systems Security Management:
  - <http://www.nerc.com/files/CIP-007-1.pdf>
- CIP-008-1 – Cyber Security – Incident Reporting and Response Planning:
  - <http://www.nerc.com/files/CIP-008-1.pdf>
- CIP-009-1 – Cyber Security – Recovery Plans for Critical Cyber Assets:
  - <http://www.nerc.com/files/CIP-009-1.pdf>

Please familiarize yourself with the above mentioned standards to be discussed at the work group kickoff meeting. Note that the formal assessment of these standards will be undertaken at a later date. To access copies of the standards, please follow the provided links.

You may also find it helpful to be familiar with the following materials:

- NIST SP800-53, Recommended Security Controls for Federal Information Systems:
  - <http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf>
- NIST SP800-82, Guide to Industrial Control Systems:
  - <http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf>
- MITRE 0700-50, Addressing Industrial Control Systems in NIST Special Publication 800-53
  - <http://homeland.house.gov/SiteDocuments/20080521141654-07244.pdf>

If you are planning to attend the upcoming SWG meeting, then please RSVP to [allison.mathews@aeso.ca](mailto:allison.mathews@aeso.ca) by Wednesday, 10 September, 2008.

*Note: The CIP standards are currently being revised by NERC. Consequently, the Security Work Group may decide to take steps to account for this uncertainty until such time as NERC has completed their revisions.*