

# NSRS Summary of Topics –August 14, 2009

---

## NERC Project 2009-18 \*\*\*\*\*

**Synopsis:** A ballot pool and pre-ballot window has opened for the NERC Project 2009-18 (“Withdraw Three Midwest ISO Waivers”). The applicable entity is a **Balancing Authority**.

The Midwest ISO is now a Balancing Authority so three NERC waivers are being withdrawn for the standards:

- Inadvertent Accounting Waiver from BAL-006 — Inadvertent Accounting
- Scheduling Agent Waiver from INT-003 — Interchange Transaction Implementation
- Enhanced Scheduling Agent Waiver from INT-003 — Interchange Transaction Implementation

Also, two standards are being revised

- BAL-006-2 — Inadvertent Interchange
- INT-003-3 — Interchange Transaction Implementation

\*\*\*\*\*

## RSDP \*\*\*\*\*

**Synopsis:** The modified Reliability Standards Development Procedure is open for a re-ballot. All entities are applicable. The initial ballot results were voided and all previous votes have been removed from the count. Voters have been asked to resubmit their votes and any applicable comments.

The modification were:

- The procedures to develop and approve of the Violation Risk Factors and the Violation Severity Levels were modified.
- National security emergencies were integrated.
- The Joint Interface Committee was dissolved.

\*\*\*\*\*

# NSRS Summary of Topics –August 14, 2009

---

## Project 2007-17 \*\*\*\*\*

**Synopsis:** Project 2007-17 (“Transmission and Generation Protection System Maintenance and Testing”) has opened for a comment period. This project is applicable to **GO, TO, & DP**. This project consolidated four existing NERC standards (PRC-005-1, PRC-008-0, PRC-011-0, and PRC-018-0) into one standard. (PRC-005-2)

This consolidated standard will allow the Protection System owner to have a time based, condition based, and/or a performance based maintenance program; the Protection System owner will have the flexibility to take advantage of different levels of monitoring.

Should the Protection System owner have a Protection System component which does not have self-monitoring alarms or if self-monitoring alarms are available and those alarms are not transmitted to a location where action can be taken for those alarmed failures, then the maintenance interval will be as short as those listed in table 1a (“Maximum Allowable Testing Intervals and Maintenance Activities for Unmonitored Protection Systems”); however, should a Protection System component have self-monitoring alarms which are transmitted to a location where action can be taken for those alarmed failures, then the maintenance intervals can be expanded to those listed in table 1b (“Maximum Allowable Testing Intervals and Maintenance Activities for Partially Monitored Protection System Components”). For example, if a protection system owner had an unmonitored protection relay, it would have to maintain this relay every 6 years, but this owner could connect this relay to SCADA or have a person check this relay daily for alarm failures, then this relay could be maintain every 12 years.

Another feature of this standard is that it more clearly delineates which generation Protection Systems will be required to be included in a maintenance program.

\*\*\*\*\*

## “Categorizing Cyber Systems – An Approach based on BES Reliability Functions” Concept Paper \*\*\*\*\*

**Synopsis:** Concept Paper to modify existing NERC Reliability CIP-002 through CIP-009 Standards pursuant to FERC order 706. All Entities are applicable. Comments and Suggestions are due September 4, 2009. These comments and suggests are to cover four specific areas of interest:

1. BES reliability functions
2. identification of BES subsystems and BES cyber systems
3. mapping of BES subsystems
4. categorization of cyber systems

\*\*\*\*\*

# NSRS Summary of Topics –August 14, 2009

---

## Order 706 B Nuclear Plant Implementation Plan \*\*\*\*\*

**Synopsis:** The Applicable entity is a Nuclear power plant. FERC's Cyber Security Order 706B told NERC to create an implementation plan for the CIP-002-1 through CIP-009-1 standards across nuclear power plants. This implementation plan is open for simultaneous commenting and balloting period to be closed on August 14, 2009.

\*\*\*\*\*

## Changes to NERC functional Model \*\*\*\*\*

**Synopsis:** The NERC Reliability Standards are based on the NERC functional model. This model along with its technical supporting document (Separate NERC email announcement) has been revised and comments on these revisions are due back August 19, 2009. All entities are applicable.

The revisions were:

- Consideration of comments from Planning Committee regarding Demand Resources function and associated responsible entities
- Review of all Planning functions and respective responsible entities
- Review of Interchange function and Interchange Authority as the responsible entity
- Review of Load Serving Entity and Distribution Provider
- Review of Terminology and Definitions for consistency with other NERC documents

\*\*\*\*\*

# NSRS Summary of Topics –August 14, 2009

\*\*\*\*\*

## Project 2009-09 CIP-001-1R2

**Synopsis:** This is a ballot for which *Covanta Energy* is requested an interpretation of *CIP-001-1 R2 (Project 2009-09)* on two points (All entities are applicable):

**Question:** Please clarify what is meant by the term, “appropriate parties.” Moreover, who within the Interconnection hierarchy deems parties to be appropriate?

**Interpretation:** CIP-001-1 R2 refers collectively to entities with whom the reporting party has responsibilities and/or obligations for the communication of physical or cyber security event information. Those entities to which communicating sabotage events are appropriate would be identified by the reporting entity and documented within the procedure required in CIP-001-1 R2.

Regarding “who within the Interconnection hierarchy deems parties to be appropriate,” the drafting team knew of no interconnection authority that has such a role.

\*\*\*\*\*

\*\*\*\*\*

**Synopsis:** The **Geomagnetic Disturbance Reference Document** which is included in the NERC Operating Manual has been updated by the Reliability Coordinator Working Group. Applicable entities are **RC, TO, TOP, GOP, and GO**.

Geomagnetic storms produced from the sun induce geomagnetically induced currents which have been known to cause the following problems on power systems:

1. Unusual noise, severe half-cycle saturation and increased VAR demand in transformers.
2. Real and reactive power swings on long transmission lines.
3. Frequency and/or voltage excursions.
4. Tripping of capacitor banks by neutral ground current.
5. Harmonic currents.
6. Hunting of automatic LTC transformers.
7. Communication system problems.
8. Oscillograph operations.
9. Operation or non-operation of protective relays.
10. Negative sequence relays alarmed.

This Reliability Guideline indicates the procedures followed when a geomagnetic disturbance is detected, the alerts which are distributed, and the centers where geomagnetic disturbances are monitored.

\*\*\*\*\*

## NSRS Summary of Topics –August 14, 2009

---

\*\*\*\*\*

**Synopsis: Project 2009-06 (“Facility Ratings”)** is open for comments.

Applicable entities are TO and GO. The SDT is asking for comments on the second draft of the FAC-008-2 (“Facility Ratings”) standard and the associated revised SAR. The recommended changes identified in the Standard Review Guidelines attached to the revised SAR and two of the three applicable FERC directives in Order 693 were made. The proposed changes to FAC-008-1 and FAC-009-1 have already been through stakeholder review and reached consensus in 2008 on all requirements except Requirement R7 developed to meet the FERC directive in Order 693 that required identification of the most limiting component of a facility and the theoretical increase in rating if the limitation were removed. Stakeholders indicated that Requirement R7 did not have a reliability-related benefit, and voted against the inclusion of a requirement to meet this directive. Thus, this revised SAR proposes the same standard that was developed and balloted in late 2008, but without Requirement R7.

\*\*\*\*\*

## NSRS Summary of Topics –August 14, 2009

---

Project 2009-13 \*\*\*\*\*

**Synopsis:** A ballot pool has opened for project **2009-13 (Interpretation of CIP-006-1 R1.1 for PacifiCorp)**. All entities are applicable. The following questions were asked and the Cyber Security Order 706 SAR drafting team submitted some responses on behalf of NERC.

**Question:** If a completely enclosed border cannot be created, what does the phrase, "to control physical access" require? Must the alternative measure be physical in nature? If so, must the physical barrier literally prevent physical access e.g. using concrete encased fiber, or can the alternative measure effectively mitigate the risks associated with physical access through cameras, motions sensors, or encryption? Does this requirement preclude the application of logical controls as an alternative measure in mitigating the risks of physical access to Critical Cyber Assets?

**Response:** For Electronic Security Perimeter wiring external to a Physical Security Perimeter, the drafting team interprets the Requirement R1.1 as not limited to measures that are "physical in nature." The alternative measures may be physical or logical, on the condition that they provide security equivalent or better to a completely enclosed ("sixwall") border. Alternative physical control measures may include, but are not limited to, multiple physical access control layers within a non-public, controlled space. Alternative logical control measures may include, but are not limited to, data encryption and/or circuit monitoring to detect unauthorized access or physical tampering.

\*\*\*\*\*

## NSRS Summary of Topics –August 14, 2009

---

Project 2009-12 \*\*\*\*\*

**Synopsis:** A ballot pool has opened for project **2009-12 (Interpretation of CIP-005-1 R4.2.2 and R1.3 for PacifiCorp)**. All entities are applicable. The following questions were asked and the Cyber Security Order 706 SAR drafting team submitted some responses on behalf of NERC.

**Question #1:** What kind of cyber assets are referenced in 4.2.2 as "associated"? What else could be meant except the devices forming the communication link?

**Response #1:** In the context of applicability, associated Cyber Assets refer to any communications devices external to the Electronic Security Perimeter, i.e., beyond the point at which access to the Electronic Security Perimeter is controlled. Devices controlling access into the Electronic Security Perimeter are not exempt.

**Question #2:** Is the communication link physical or logical? Where does it begin and terminate?

**Response #2:** The drafting team interprets the data communication link to be physical or logical, and its termination points depend upon the design and architecture of the communication link.

**Question #3:** Please clarify what is meant by an "endpoint"? Is it physical termination? Logical termination of OSI layer 2, layer 3, or above?

**Response #3:** The drafting team interprets the endpoint to mean the device at which a physical or logical communication link terminates. The endpoint is the Electronic Security Perimeter access point if access into the Electronic Security Perimeter is controlled at the endpoint, irrespective of which Open Systems Interconnection (OSI) layer is managing the communication.

**Question #4:** If "endpoint" is defined as logical and refers to layer 3 and above, please clarify if the termination points of an encrypted tunnel (layer 3) must be treated as an "access point? If two control centers are owned and managed by the same entity, connected via an encrypted link by properly applied Federal Information Processing Standards, with tunnel termination points that are within the control center ESPs and PSPs and do not terminate on the firewall but on a separate internal device, and the encrypted traffic already passes through a firewall access point at each ESP boundary where port/protocol restrictions are applied, must these encrypted communication tunnel termination points be treated as "access points" in addition to the firewalls through which the encrypted traffic has already passed?

**Response #4:** In the case where the "endpoint" is defined as logical and is  $\geq$  layer 3, the termination points of an encrypted tunnel must be treated as an "access point." The encrypted communication tunnel termination points referred to above are "access points."

\*\*\*\*\*