

NSRS Summary of Topics –December 18, 2009

Key for far left-hand side of summary

Symbol	NSRS Deadline To
“V”	Vote
“B”	Enter ballot
“C”	Submit comments

Project 2009-13 Recirculation Interpretation of CIP-006-1 R1.1 By PacifiCorp

V 12/21/09

A recirculation ballot window has opened for the project [2009-13](#). (“**Interpretation of CIP-006-1 R1.1 for PacifiCorp**”) Originally, the initial ballot reached quorum (84.92%) and was approved (79.04%) but negative comments were received.

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, motion 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.

Project 2009-03 Emergency Operations

C 01/15/10

Drafting Team Nominations are being received to serve on the Emergency Operations SAR Drafting Team. (Due 12/18/09) A proposed SAR and white paper have also been posted for a 30-day comment period. Applicable entities are: **RC, BA, TOP, TSP, DP, GOP, PSE, & LSE.**

The [SAR and white paper cover](#) the merging of four standards: EOP-001 (“Emergency Operations Planning”), EOP-002 (“Capacity and Energy Emergencies”), EOP-003 (“Load Shedding Plans”), & IRO-001 (“Reliability Coordination - Responsibilities and Authorities”).

This project will require close coordination with two other drafting teams – the Operations Communications Protocols SDT and the Reliability Coordination SDT.

NERC project 2007-02 Operating Personnel Communications Protocols

C 01/15/10

A comment period has opened for the NERC project [2007-02](#) (“Operating Personnel Communications Protocols”). Applicable entities are: **TOP, TO, BA, RC, GOP, DP, TSP, & LSE.**

NSRS Summary of Topics –December 18, 2009

Key for far left-hand side of summary

Symbol	NSRS Deadline To
“V”	Vote
“B”	Enter ballot
“C”	Submit comments

The drafting team reviewed communication protocols in other NERC standards and considered the use of alert level guidelines and three-part communications to achieve consistency across regions. The proposed standard is designed to ensure that reliability-related information is conveyed effectively, accurately, consistently, and timely to ensure mutual understanding by all key parties, especially during alerts and emergencies. This new standard proposes new terms such as **Communications Protocol, Three-part Communication, & Interoperability Communication.**

Project 2009-24 Interpretation of EOP-005-1 R7 By FMPA

B 01/05/09

A pre-ballot window has opened for the interpretation of [EOP-005-1 R7](#) by Florida Municipal Power Agency (FMPA). Applicable entities are **BA & TOP.**

The FMPA asked the following questions and the System Restoration and Blackstart drafting team (NERC project 2006-03) has respond to these questions, below.

Question #1 - What is meant by the phrase “verify the restoration procedure” and by the term “simulation” in requirement R7?

Response to Question #1 - Verifying the restoration procedure means establishing that the restoration procedure is technically sound and can progress as planned. A restoration plan is typically broken down to its restoration levels, tasks, and basic operating actions (opening/closing breakers, raising/lowering transformer taps, adjusting voltage and frequency set points, starting motors, etc). Usually, some activities cannot begin until others have been completed, so the restoration procedure lists the predecessor of each activity. The purpose of verifying the restoration procedure is to determine that the entire plan is broken down into some logical order that reduces the risk of overlooking any essential operation.

Verifying Restoration by Simulation: With each significant restoration action, concerns are with exceeding high/low operating limits. Various analytical tools are used to verify safe operations by engineers, operators, and instructors/trainees during different operating conditions, such as pre-disturbance condition, post-disturbance status, and actual emergency operating condition. These tools include power flow, transient stability, long-term dynamics, voltage transients, short circuit, electromagnetic transient programs, etc.

For a small TOP with no blackstart capability, the technical aspects of the smaller TOP's restoration plan may be incorporated into the plan of a larger TOP and may be included in the larger TOP's testing or simulation. The requirement does not state that every TOP has to physically perform simulation or testing; the requirement only mandates verifying the plan with simulation or testing. Another TOP, the Reliability Coordinator, or a contractor could perform testing or simulation on behalf of the smaller TOP.

Question #2 - For a TOP without any blackstart facilities in its restoration plan, can exercises and tabletop drills be used to meet Requirement R7 by “verifying the restoration procedure” through tabletop “simulations?”

Response to Question #2 - Based on the reference document quoted above, the drafting

NSRS Summary of Topics –December 18, 2009

Key for far left-hand side of summary

Symbol	NSRS Deadline To
“V”	Vote
“B”	Enter ballot
“C”	Submit comments

team interprets that tabletop exercises can meet some of the requirements but cannot be used to meet the simulation requirements.

Project 2009-25

Interpretation of BAL-001-01 & BAL-002-0 By BPA

B 01/05/09

A pre-ballot window has opened for the interpretation of [BAL-001-0.1a R1 & BAL-002-0 R4](#) by Bonneville Power Administration (BPA). Applicable entities are **BA & RSG**.

The BPA asked the question and the Balancing Authority Controls drafting team (NERC project 2007-05) has responded.

Question #1 - When responding to a disturbance as described in BAL-002 R4, BPA questions whether the "ACE" referenced in the standards is intended to be the "control ACE" used in AGC, or the "raw ACE" referenced in BAL-001? Also, can the "raw ACE" referenced in BAL-001 include the ADI offset?

Response to Question #1 - The drafting team interprets that the ACE referenced in BAL-002-0 Requirement R4 is ACE as defined in BAL-001-0.1a Requirement R1 ("raw ACE" or "reporting ACE").

As described in the definition of Reserve Sharing Group, if an entity experiencing a Disturbance is scheduling energy from an Adjacent Balancing Authority to aid recovery and ramping it in over a period faster than the supplying party could reasonably be expected to load generation, then the Areas become a Reserve Sharing Group for the purposes of evaluating disturbance control performance. Consequently, for the purposes of determining ACE recovery in response to a Reportable Disturbance, the reporting entity must account for all entities that responded to the Disturbance. In cases where an entity experiencing a Reportable Disturbance (either with a single Balancing Authority or with a Balancing Authority that is part of a Reserve Sharing Group) is part of an ACE diversity interchange (ADI) group where ADI is implemented in real time and is implemented such that all ADI participants' ADI adjustments net to zero, then the accumulated ACE of all members of the Reserve Sharing Group, as well as all members of the ADI who are not Reserve Sharing Group members, shall be utilized when computing the collective ACE used for evaluation of the Reserve Sharing Group's performance to meet the Disturbance Control Standard (DCS). The Balancing Authority or Reserve Sharing Group with the Disturbance remains the responsible entity for the purposes of compliance to the NERC standards. The reason for using the collective ACE values for all participants (Reserve Sharing Group members and ADI participants which are not members of the Reserve Sharing Group) when determining the collective ACE is to effectively remove any ADI impacts to ACE equations. As NERC does not have any standards related to ADI, and ADI implementation can vary widely, it is unclear whether or not ADI should be included in the ACE described in BAL-001-0.1a. NERC has other options for addressing this question, such as the standards development process, which includes a special procedure for variances, or the Joint Registration Organization provision of the Organization Registration and Certification Program.

Project 2009-26

Interpretation of CIP-004-1 R2-R4 By WECC RC

B 01/06/09

A pre-ballot window has opened for the interpretation of [CIP-004-1 R2-R4](#) by Western Electricity Coordinating Council RC. **Applicable entities are All.**

NSRS Summary of Topics –December 18, 2009

Key for far left-hand side of summary

Symbol	NSRS Deadline To
“V”	Vote
“B”	Enter ballot
“C”	Submit comments

The Cyber Security Order 706 SAR drafting team (Project 2008-6) has responded.

Question: The WECC RC seeks clarification on the definition of “authorized access” as applied to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access be considered supervision?

Response: The drafting team interprets that a vendor may be granted escorted physical access to Critical Cyber Assets; however, for a vendor to be granted authorized cyber access, the vendor must complete the risk assessment and training as required by CIP-004-1 Requirement R2. CIP-003-1 Requirement R3 permits exceptions to an entity’s cyber security policy, such as for an event requiring emergency access. It is recognized that the cited question and answer from the Frequently Asked Questions CIP-004-1 Cyber Security – Personnel & Training document states that “...some form of supervision is appropriate for anyone with cyber access who has not been subjected to a personnel risk assessment and appropriate training.” However, this particular guidance should be revisited. For purposes of CIP-004-1, there is no way to provide effective escorted or supervised cyber access to ensure that the actions of vendors who have not received the cyber security training and a personnel risk assessment do not harm the integrity of a Critical Cyber Asset or the reliability of the bulk power system during that electronic access. It is further noted that an FAQ is not a standard, and cannot create or dilute the language of the standard itself.

Project 2009-06 Facility Ratings

B 01/12/09

A ballot pool and pre-ballot Window has opened for the NERC project [2009-06](#) (“Facility Ratings”). **Applicable entities are TO & GO.**

This consolidated standard (which merges FAC-008-1 and FAC-009-1) was developed in 2008. This project has been initiated to revise the Generator Owner requirements to provide greater clarity of the Generator Owner responsibilities and options for developing facility rating documentation. Plus, the compliance elements will be revised to conform to changes made to the requirements for the Generator Owner.