SERC RELIABILITY CORPORATION

Evaluation | Analysis | Assistance | Operating Experience

2019 Spring Compliance Seminar

This document provides SERC staff responses to questions asked by entities. The information provided herein is intended, on its date of posting, to provide guidance to the industry. Actions based on this information shall have no standing for the purpose of contesting or mitigating any findings of noncompliance by SERC. Compliance depends on a number of factors including the precise language of the Standard, the specific facts and circumstances, and the quality of evidence. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time.

1. EOP-004-4 - Attachment 1: Reportable Events

Uncontrolled loss of firm load resulting from a BES Emergency

Uncontrolled loss of firm load for ≥ 15 minutes from a single incident: ≥ 300 MW for entities with previous year's peak demand ≥ 3,000 MW OR ≥ 200 MW for all other entities

As it applies to Distribution Providers:

Question 1.) For Joint Registration Organizations does the ≥ 300 MW or 200 MW threshold apply to the JRO Entity or the individual Non-Registered Entity Members?

For Joint Registration Organizations the ≥ 300 MW or 200 MW threshold would apply to the aggregate of the individual Non-Registered Entity Members.

1.a) Further if there are UFLS-Only DP Non-Registered Entity Members in the JRO, does the threshold apply to those members?

No, this standard only applies to the RC, BA TO, TOP, GO, GOP and DP. Most if not all of the UFLS systems are installed on Non-BES elements. UFLS-Only DPs are subject only to the PRC-006-1 Reliability Standard (as modified from time to time) under the DP applicability and any Reliability Standards that specifically reference UFLS-Only DPs in the applicability section. Other standards applicable to DPs are not applicable to UFLS-Only DPs.

Question 2) For large scale weather events or natural disasters, should the group of resulting outages be treated as a single incident or should each damaged distribution feeder be considered a separate incident?

This should be treated as a single incident under Transmission Loss or Loss of Firm Load for 15 minutes.

2.a.) If treated as a single incident, should event start and end times reflect the period of time where outages cumulatively surpass the ≥ 300 MW or 200 MW threshold?

Yes, the start time should reflect the period of time when the event passed the threshold. The stop time should be when the potential for further disruption of the system from this event no longer existed. You could provide updates in the interim as to the situation.

2. **The proposed CIP-002-6 standard adds an "aggregate weighted value" in Attachment 1, section 2.12. For some entities, this will reduce their control center's status from a Medium-Impact to Low-Impact. Will such entities be audited on or expected to comply with CIP Medium-Impact requirements after this new version of the standard is approved, but is still pending enforceability? If so, entities could be required to make significant investments due to other evolving CIP requirements for Medium-Impact BCS for the short time prior to the new version being effective."**
   This version of the standard is still in "draft" format so it will not be put into scope until it is approved by FERC and according to the implementation plan set by NERC. Standards in force are effective until they are retired, unless otherwise specified in the implementation plan.

3. **Please clarify when a Registered Entity would be accountable for meeting the requirements of a Standard or requirement depending on the effective date when the Registered Entity has begun efforts to prepare its organization for a requirement subject to future enforcement. For example, a NERC Standard has phased in requirements, and one of the requirements will be effective November 1, 2019. The requirement requires a process and/or procedure in place to achieve certain outcomes. The Registered Entity is aware they will be subject to the requirement effective November 1, 2019 and implements processes, procedures, and tools in place May 1, 2019 to provide time to practice, review documentation for sufficiency, and to make modifications and train Registered Entity personnel as may be necessary in order to ensure the Registered Entity will be compliant beginning November 1, 2019.**

   In an audit for this requirement, will the Registered Entity be accountable for and held to compliance for any time prior to the NERC requirement effective date of November 1, 2019 even if the entity set an effective date for their organization months prior to the NERC effective date?

   A registered entity will not be assessed non-compliant and penalized financially for any requirement for any period of time prior to the Effective Date of FERC approval. A requirement is not mandatory and enforceable prior to the Effective Date.

Effective Date: The date upon which the Reliability Standard goes into effect. On the Effective Date of a Reliability Standard, the Reliability Standard becomes mandatory and enforceable, and applicable entities are responsible for compliance with the Requirements in the Reliability Standard. An Implementation Plan may also provide for a delayed or "Phased-In Implementation Date" for specific Requirements (or parts) contained within the Reliability Standard for which a longer implementation period is appropriate.

Phased-In Implementation Date (if applicable): The date, following the Effective Date of the Reliability Standard, upon which implementation of a specific Requirement (or part) is first required, as specified in the Implementation Plan for the Reliability Standard. In some instances, there may be a need to provide entities additional time beyond the Reliability Standard's Effective Date to comply with a particular Requirement (or part). In those instances, the Implementation Plan will provide a Phased-In Implementation Date specific to that Requirement (or part). The "Phased-In Implementation Date" thus represents the later date that entities must begin complying with that particular Requirement (or part).

4. **Regarding PRC-005, what is required to establish the start of interval for a component? For a new component selected for an audit, what if anything, are we required to show an auditor to prove that we met the requirements of PRC-005? What are we required to show an auditor as proof that all the activities required by the standard have been completed?**

   The initial due date for maintenance should be based upon when a Protection System was tested and should include all maintenance activities that are required by the standard for that component. Alternatively, an entity may choose to use the date the commission testing of the Protection System component is completed and placed into service as the starting point in determining its first maintenance due dates. Whichever method is chosen, for newly installed Protection Systems the components should not be placed into service until minimum maintenance activities listed on the applicable tables have taken place. This standard does not establish requirements for commission testing. Commission testing includes all testing activities necessary to conclude that a Facility has been built in accordance with design. PRC-005-6 assumes that thorough commission testing was performed prior to a Protection System being placed in service. The commission testing activities will not necessarily correlate directly with the maintenance activities required by the standard.

   Evidence required for a new device would be completed testing records that show at a minimum that all maintenance activities included in the applicable maintenance table were tested successfully and completed. Some of these could include commissioning test records, dated maintenance records, dated maintenance summaries, dated check-off lists, dated inspection records, or dated work orders.

5. **Regarding PRC-005, SERC has taken the position that we have to show milestones and demonstrate progress on activities to deal with unresolved maintenance issues. Is this required by NERC overall, or is SERC at liberty to have more restrictive requirements?**

   SERC audits for compliance in accordance with and subject to language of the standard. The requirement does not state how quickly a corrective action for unresolved maintenance issues needs to be resolved. Completed milestones is one way for the entity to demonstrate their efforts to correct identified Unresolved Maintenance Issues.

   There can be any number of supply, process and management problems that make setting repair deadlines impossible. The SDT specifically chose the phrase "demonstrate efforts to correct" (with guidance from NERC Staff) because of the concern that many more complex Unresolved Maintenance Issues might require greater than the remaining maintenance interval to resolve (and yet still be a "closed-end process"

   R5: Each Transmission Owner, Generator Owner, and Distribution Provider shall demonstrate efforts to correct identified Unresolved Maintenance Issues.

   M5: Each Transmission Owner, Generator Owner, and Distribution Provider shall have evidence that it has undertaken efforts to correct identified Unresolved Maintenance Issues in accordance with Requirement R5. The evidence may include, but is not limited to, work orders, replacement Component orders, invoices, project schedules with completed milestones, return material authorizations (RMAs) or purchase orders.

   However, if this question is geared toward Enforcement, the ROP requires milestones if mitigation will not be complete within three months of the submission of the Mitigation Plan.

6. **What is SERC's expectation for completion of an RSAW for a Standard Requirement that is currently not enforceable? Request was made as part of an audit, but SERC stressed could not be found non-compliant with the requirement.**

   SERC may request completion of an RSAW for a Standard Requirement that is currently not enforceable. For example, a standard requirement that is mandatory and enforceable at any time during the audit period, but currently not enforceable, may be reviewed and an applicable entity found compliant or non-compliant with the standard requirement. SERC won't audit for standards with future enforceable dates, but may go back during the audit period.

7. **EOP-004 SERC notification number appears to have changed, as published in SERC newsletter. Given the Requirement 1 for entities to notify SERC, was there any other announcement of the number change? Did it go to Primary Compliance Contacts?**

When did it change? Did the Regional Criteria for Disturbance Reporting document change? Would you provide the email address and phone number?

The primary methods for communication of EOP-004 related events to NERC is listed in Attachment 1 of EOP-004. NERC in turn forwards all SERC related events to SERC. The SERC Regional Criteria request that SERC also be included in the initial notification as an added redundancy measure. The SERC email address for notification has not changed: email: reporting_line_sit@list-serc1.org. The SERC phone number did change and this information was distributed to the SERC Region via the January 2019 SERC newsletter. The new number is 704-405-8700.

8. **What are expectations for Internal Controls in an audit? If not part of Standards, the depth of information requested by auditors seems excessive. If not part of Standards, how can the information provided be considered "evidence". How will this information be considered in future audits? For entities new to SERC that may have provided internal controls information for a different Region, how far ahead will SERC provide internal controls questions to allow the entity to prepare?**

   NERC has directed the Regional Compliance Enforcement Agencies (CEA) to obtain an understanding of internal controls through inquiries, observations, inspection of documents and records, review of other CEA staff reports, and direct tests. SERC's approach for Internal Controls during an audit comprise the following:

   - *An initial set of General Internal Control Questions will be sent out on a Request for Information (RFI) document that includes the initial set of Logistics questions. This RFI will be included in the Audit Notification Package that is sent to the entity 120 days prior to the start of the On-Site Audit week. Answers to these initial questions will provide the auditor(s) a general understanding of the entities internal control program or activity, the maturity level of the program, and some knowledge about the internal control processes in place prior to the start of compliance monitoring activities.*
   - *In an effective compliance program, a registered entity's internal controls provide reasonable assurance that its compliance obligations are met. Consideration of internal controls in auditing is a standard practice. As such the audit team needs to ensure documentation of the internal controls that support compliance of the standard and requirement are recorded in the RSAW. This portion of the internal controls process will take place during off site review of the initial evidence the entity provided to support compliance, during review of sampling requests information and evidence provided and through review of subsequent data requests information and evidence. Auditors will document a summary of internal controls identified during this review in the RSAW.*
   - *During on-site discussions with SME for standards and requirements that are still open the audit team will include additional internal control questions that are applicable to that specific standard and requirement. The responses and evidence provided will be cited in the RSAW as additional "stacking" evidence.*

- *Also during the on-site audit week, the audit team will schedule an Internal Controls discussion with the entities PCC, Compliance Department, Internal Auditing Department, etc. to gain further understanding about the entities internal control program. Some common areas of discussion could include how the entity identified key risk and controls for high risk standards and requirements, whether the entity has conducted testing of the controls for effectiveness in mitigating risks, gaps in internal controls and how the entity addressed and eliminated the gaps and if there are any Quality Assurance or Control reviews being performed. The audit team will also discuss the entities future plans and their way ahead for internal controls. The auditors will provide feedback to the registered entity on internal controls, such as recommendations for improvements, discussions around best practices, areas of concerns.*
- *This process will give the auditors sufficient information to make decisions on the effectiveness of internal controls and to determine how they may influence changes to the registered entity's COP. Review of an entities internal control program could result in targeted BES reliability risk focused scoping, reduction in the amount of sampling required in future engagements, improved risk and control awareness and enhanced attainment of BES reliability.*

9. **Comment - EISAC has been set up as the industry "one-stop-shop" for reporting. Perhaps EISAC could be leveraged more fully for industry event reporting.**

   Comment; no response necessary.

10. **How does SERC treat the "cascading" impact of violations; i.e., is a violation given only on the "parent" Requirement or also for each sub-requirement? Differences are seen between Regions.**

    SERC generally calls out the "parent" violation and addresses any resulting "child" violations in mitigation. Given the statement that there are differences between the Regions, SERC will work with the other Regions and NERC to determine what differences exist and reach a common approach going forward.

11. **Regarding CIP-003 physical access to low facilities or low assets, is there an expectation to have multiple barriers "defense-in-depth" approach? What would constitute a breach of a physical barrier? How are fence-line barriers such as rail passes, normal day-time vehicle traffic treated when such barriers must be breached during normal course of business?**

    The expectation is to see the plan each Entity utilizes to control physical access, based on need as determined by the Entity.

12. **Regarding CIP-003 physical security, many Low Impact Generation sites have only the fence between the public and some BES Cyber Systems; e.g., they can be located within an open boiler or other exterior Balance of Plant Items located within the site boundary. Most of these types of Generation have the core of their network systems locked in relay rooms and control rooms but do have sensor devices located externally. What is the audit expectation?**

    The audit expectation is that the Entity will follow its prescribed physical access control plan, applicable to the site in question.

13. **Concerning audit scope, if the audit letter lists only the latest version of a Standard in scope but the audit period goes back prior to the current Standard, is it implied that the prior versions are also in-scope? Is SERC looking for all versions of procedures that an entity had to cover all the versions of the Standard?**

    Yes. SERC will look at the current version, and if there is a problem, we would look back to the previous version. This approach would include versions of procedures as well.

14. **Are the expectations for completing a TOP Control Center certification for a non-TOP high impact Control Center the same as for TOP Control Center? This is due to replacement of the current non-TOP high impact Control Center.**

    Yes. There are examples across the ERO where the registered TOP delegates tasks to local control centers. In these instances changes to the local control centers can trigger a Certification activity of the registered TOP. The construction of a new local control center would be one of the triggers. The TOP tasks being performed at the new facility would need to be demonstrated.

15. **Does a new back-up Control Center need to be certified prior to being operational?**

    Yes. This is also one of the triggers for a Certification activity of the TOP registration. The TOP tasks being performed at the new facility would need to be demonstrated.

16. **Does the RE audit storage server or data server as identified BES Cyber System storage information?**

    SERC has applied a set of protections that goes beyond the confidentiality protection required by the CIP standards. Below are the security controls associated with the PEI server:

- *Resides in a DMZ;*
- *Two Factor authentication is required;*
- *All data is AES encrypted.*

17. Within CIP-010-2 R1 for High Impact BES Cyber Systems, is Part 1.4.2 "*Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and*" and also requirement 1.5 for High Impact BES cyber systems. "*Where technically feasible, for each change that deviates from the existing baseline configuration: 1.5.1. Prior to implementing any change in the production environment, test the changes in a test environment or test the changes in a production environment where the test is performed in a manner that minimizes adverse effects, that models the baseline configuration to ensure that required cyber security controls in CIP-005 and CIP-007 are not adversely affected; and*". Does 1.5.1 override/take the place of 1.4.2? Or must both be performed? If an entity has already verified there is no impact in a test environment, why re-perform in the live environment?

Part 1: Sequentially, the steps that the Entity should perform for high impact BES Cyber System would be 1.4.1, 1.5.1, 1.5.2. Then the Entity would perform the change and perform 1.4.2 and 1.4.3.

Part 2: The verification is to ensure that the observed result in the low-risk test environment of 1.5.1 is a repeatable result for 1.4.2 in production after the change is implemented in production.

18. Clarification of Audit Period?

Every Registered Entity has to be compliant with all approved NERC Reliability Standards at all times, per your registered functions.

In accordance with Appendix 4C to the NERC Rules of Procedure, the Registered Entity's data and information must show compliance with the Reliability Standards that are the subject of the Compliance Audit for the entire period covered by the Compliance Audit. The Compliance Enforcement Authority will indicate the beginning and end date of the audit period in its notice of the Compliance Audit (Audit Notification Letter – ANL). The ERO has agreed on a common audit period across all regions. The audit period begins the day after you receive your previous Audit Notification Letter (ANL), and ends on the day you receive the next ANL.