

# NERC

NORTH AMERICAN ELECTRIC  
RELIABILITY CORPORATION

## NERC Regional Entity Audit of SERC Reliability Corporation

Prepared by Jacqueline Power

to ensure  
the reliability of the  
bulk power system

116-390 Village Blvd., Princeton, NJ 08540  
609.452.8060 | 609.452.9550 fax  
[www.nerc.com](http://www.nerc.com)

# Table of Contents

---

<b>Chapter 1 – Executive Summary</b> .....	<b>1</b>
<b>Best Practices (for Consideration)</b> .....	<b>3</b>
SERC Compliance Duty Person (Screener):.....	3
Single Point of Contact (SPOC) .....	3
Compliance Enforcement Peer Review Meetings .....	3
Audit “Scribe” Position.....	4
Multiple Reviews/Checks and Balances - Compliance Audit and Enforcement Staff.....	4
Strong Team Approach.....	4
Staff Guide for Data Management and Confidentiality.....	4
SERC’s Portal.....	5
<b>Chapter 2 – Background</b> .....	<b>6</b>
<b>Program Development</b> .....	<b>6</b>
<b>Chapter 3 – Audit Process</b> .....	<b>7</b>
<b>Compliance and Certification Committee Participation</b> .....	<b>7</b>
<b>Pre-Audit</b> .....	<b>7</b>
<b>Off-Site Audit Process</b> .....	<b>7</b>
<b>On-Site Audit Process</b> .....	<b>8</b>
Exit Presentation .....	<b>9</b>
<b>Security and Confidentiality of Audit Evidence</b> .....	<b>10</b>
<b>Chapter 4 – Financial and Budget Management</b> .....	<b>11</b>
<b>Background</b> .....	<b>11</b>
<b>Discussion of Review</b> .....	<b>11</b>
<b>Conclusion</b> .....	<b>11</b>
<b>Chapter 5 – Information Systems</b> .....	<b>12</b>
<b>Discussion of Review</b> .....	<b>12</b>
Data Management, Security and Access Controls .....	12
Classification of Data.....	12
Data Transmittal.....	13
Data Backup and Recovery.....	13
<b>Conclusion</b> .....	<b>13</b>
<b>Chapter 6 – Compliance Audit Validation</b> .....	<b>14</b>
<b>Discussion of Review</b> .....	<b>14</b>
<b>Conclusion</b> .....	<b>14</b>

**Appendix A – AUP Exceptions to the Rules of Procedures, Delegation Agreement and Other..... 15**

**V – Reporting to NERC..... 15**

**VIII – Compliance Activities..... 15**

**XVI – ERO Functional Requirements ..... 16**

**Appendix B – AUP Exceptions ..... 17**

**III – Independence ..... 17**

    Internal Regional Entity (RE) Governance and Conflict of Interest..... 17

    Conflict of Interest by External Parties..... 17

**VI – Registration ..... 17**

**VIII – Compliance..... 18**

**XIII – Mitigation Plans..... 18**

**Appendix C – AUP Procedures List..... 20**

## Chapter 1 – Executive Summary

In accordance with the Federal Energy Regulatory Commission’s (FERC) Order No. 672, the North American Electric Reliability Corporation (NERC) developed a program to audit the Regional Entities adherence to the Rules of Procedures (RoP), the Compliances Monitoring and Enforcement Program (CMEP) and the requirements of the Regional Delegation Agreement (RDA). This effort was pursuant to the Commission’s direction contained in Paragraph 773.<sup>1</sup> Additional requirements concerning the Regional Entity Audit Program attributes are contained in the RoP Section 402.1.3.<sup>2</sup>

Based on the NERC Board of Trustees’ (BOT) recommendation, NERC partnered with an independent auditing firm, Crowe Horwath, LLP (Crowe) to develop the procedures and perform the Regional Entity Audit Program. NERC determined an attestation of agreed-upon procedures (AUPs)<sup>3</sup> was the best vehicle for meeting its responsibility as outlined by the Commission. The Crowe endeavor was coupled with NERC staff performing areas requiring technical subject matter expertise.

NERC staff performed assessments in the following three areas: 1) information systems (Regional Entity processes for maintenance and control of data security); 2) audit validation (validation of the results of a compliance audit performed by the Regional Entity on one of its registrants); and 3) financial and budget management (a review of the Regional Entity’s financial records).

The NERC Regional Entity audit of SERC Reliability Corporation’s (SERC) adherence to its delegated functions occurred over a four-week time period. Based on lessons learned from the

---

<sup>1</sup> See Rules Concerning Certification of the Electric Reliability Organization; Procedures for the Establishment, Approval and Enforcement of Electric Reliability Standards, FERC Stats. & Regs., ¶ 31,204 at P 773 (“Order No. 672”), *order on reh’g*, FERC Stats. & Regs. ¶ 31,212 (2006) (“Order No. 672-A”) (“We contemplate that a compliance audit of the ERO would typically involve an examination of the ERO’s ongoing compliance with statutory and regulatory criteria for certification and its performance in carrying out its responsibility to oversee the compliance with and enforcement of Reliability Standards. The Commission, however, maintains the flexibility to determine the applicable scope of a particular audit. The Final Rule eliminates the proposed periodic Commission compliance audit of each Regional Entity. Instead, we require the ERO periodically to audit each Regional Entity’s ongoing compliance with relevant statutory and regulatory criteria and performance in enforcing Reliability Standards and report the results to the Commission.”).

<sup>2</sup> See NERC Rules of Procedure at § 402.1.3 (“Regional Entity Program Audit - At least once every three years, NERC shall conduct an audit to evaluate how each regional entity compliance enforcement program implements the NERC Compliance Monitoring and Enforcement Program. The evaluation shall be based on these rules of procedures, the delegation agreement, approved regional entity annual compliance enforcement program annual implementation plans, required program attributes, and the NERC compliance program procedures. These evaluations shall be provided to the appropriate ERO governmental authorities to demonstrate the effectiveness of each regional entity.”).

<sup>3</sup> An attestation of an agreed-upon procedure is an engagement relating to agreed-upon procedures (criteria for auditing) to specified elements or accounts. Agreed-upon procedure is an engagement with an accounting firm that is hired to issue a report of findings (attestation) based on specified criteria. The user of the report, in this case NERC agree upon the procedures to be conducted by the accountant that NERC believes are suitable to the requirements. NERC takes responsibility for the adequacy of the procedures. In this engagement, the accountant does not express an opinion or negative assurance. Instead, the report is in the form of procedures and findings.

audit of Reliability *First* Corporation, the SERC audit incorporated an off-site and an on-site week. The off-site audit was held at Crowe's offices in Oakbrook, Illinois the week of June 1, 2009. One observer from the FERC, representing the Office of Electric Reliability (OER) was present.

The on-site audit was held at the SERC headquarters the week of June 15, 2009. Two observers from the FERC, representing the Office of Electric Reliability (OER) and the Office of Enforcement (OE), were present for the audit. A Compliance and Certification Committee (CCC) representative from National Grid participated as an observer. Details of the audit activities are in Chapter 3 of this report.

NERC staff validated the results of an audit SERC performed on one of its registered entities at the SERC offices the week of May 28<sup>th</sup>, 2009. NERC staff assessed SERC's processes and procedures for maintenance and control of data security the week of June 8<sup>th</sup>, 2009. SERC's staff was very accommodating to the needs of the audit team throughout the audit process. SERC provided all information requested prior to or by the due date. SERC worked diligently to provide additional information requested by the audit team prior to or by the due date specified.

There were 16 exceptions to the AUPs criteria noted, of which five were identified as exceptions to stated requirements. The attestation of the AUPs performed by Crowe is provided in a separate report.

Appendix A and B of this report contain the exceptions to the AUPs noted by Crowe. Appendix A includes exceptions relating to non-adherence to the RoP, Delegation Agreements, or other NERC guidance or direction documents. Appendix B includes exceptions that do not necessarily constitute non-adherence to the RoP and delegation agreements. For example, per the NERC CMEP § 3.4.1, Compliance Violations Investigation Process Steps, a Regional Entity is required to report to NERC within two business days, its decision to initiate a compliance violation investigation; however, documentation of its assessment and determination to initiate the investigation is not required. The lack of documentation in this example makes it difficult for the auditors to determine adherence to the requirement. From an auditing perspective and based on the American Institute of Certified Public Accountants (AICPA) standards, it is clear an action was performed when there is documentation of the action, *i.e.*, checklist, sign-off with date specified, etc., and subsequent documentation the entity met its timeline.

There were no deficiencies noted by NERC staff in the areas of information systems, compliance audit validation, or SERC's financial and budget management. NERC offered four recommendations to SERC as improvement items relating to information systems. Details regarding each area assessed by NERC are contained in subsequent sections of this report.

## **Best Practices (for Consideration)**

This is the second audit performed by NERC of a Regional Entity. Classification of best practices at this time is somewhat premature, the NERC audit team noted several areas in which items should be considered as a Regional Entity best practice:

1. 24/7 oversight of compliance issues via the use of a Compliance Duty Person (Screener);
2. Compliance Enforcement Single Point of Contact (SPOC);
3. Compliance Enforcement Peer Review Meetings;
4. Audit “Scribe” Position;
5. Multiple reviews with checks and balances in place for compliance enforcement and audit deliverables;
6. Strong team approach for determination of SERC’s compliance enforcement and audit decisions;
7. Staff Guide-Data Management and Confidentiality; and
8. SERC Portal.

### **SERC Compliance Duty Person (Screener):**

SERC uses a dedicated “screener duty” position which maintains 24/7 monitoring of incoming compliance information, via e-mails, Department of Energy OE 417 form submittals, and registrant submittals to the web-based application portal system. The screener reviews NERC, FERC and other Regional Entities Web sites for relevant news items. Identification of a possible alleged violation results in the screener duty person assessing the risk to reliability. If a risk to reliability is identified, the screener duty person immediately contacts the Manager of Compliance Enforcement.

The screener duty person creates database entries and folders for all possible alleged violations. The information gathered is shared with the enforcement and audit staff during the next daily meeting. The screener duty is a rotational position shared between the enforcement and the audit staff.

### **Single Point of Contact (SPOC)**

SERC assigns one person from its enforcement staff as a SPOC for each possible alleged violation. This staff member is the owner of the possible alleged violation from the initial notification until final resolution. The SPOC assesses the registered entity’s registration status compared to the applicability of the violated reliability standard and performs a preliminary determination. The SPOC develops a basis for the determination of the alleged violation and provides this assessment for review to enforcement peers for discussion during the compliance enforcement peer review meetings.

### **Compliance Enforcement Peer Review Meetings**

The SERC incorporates a peer review process. Members of the enforcement staff review the enforcement SPOC(s) recommendations for all compliance actions.

The enforcement staff provides input to determine final resolutions for violations, mitigation plans, and penalty determinations. Enforcement peer review sessions are held on a regularly scheduled basis via conference calls and web-based sessions.

### **Audit “Scribe” Position**

SERC compliance audit program employs the use of a “scribe” position. The scribe is considered the subject matter expert for the audit being performed. The scribe is the owner of the Reliability Standard Audit Worksheets (RSAWs). Duties include confirming the auditors are using the current RSAWs and verifying the RSAWs are completed properly. The scribe develops the report for the compliance audit. This position is separate from the Audit Team Lead (ATL).

### **Multiple Reviews/Checks and Balances - Compliance Audit and Enforcement Staff**

SERC’s compliance process incorporates multiple reviews, resulting in a check and balance hierarchy similar to what is employed in the nuclear industry. For example, for compliance audits, the ATL performs a review of the draft report. The Manager of Compliance Audits performs a review prior to sending it to the registered entity. The ATL and Manager of Compliance Audits perform another review prior to finalizing the public and non-public audit report. The Vice President and Director of Compliance reviews and approves the audit reports prior to the publication. This process is performed in other compliance enforcement activities. The Manager of Compliance Enforcement reviews and approves all enforcement decisions and then forwards the decision to the Vice President and Director of Compliance for final approval.

### **Strong Team Approach**

SERC uses the peer review (discussed previously) and consensus process for all aspects of its compliance processes. Although this appears to be very time intensive, the team approach allows for consistency in the determinations throughout the entire compliance department along with promoting consistency of findings between registered entities. When the President and CEO, and vice president and director of compliance were queried as to what aspect of their operation they were the most proud of, both replied the caliber and dedication of their staff. SERC fosters the environment of team work among its staff.

### **Staff Guide for Data Management and Confidentiality**

SERC developed an internal procedure titled, “Staff Guide - Data Management and Confidentiality.” This procedure provides guidance to its compliance staff concerning the handling of sensitive data. Included in the procedure is a concise attachment which is a quick reference guide. The reference guide provides explanations and instructions for types of documents and how to treat documents depending on classification and state (whether the documents are in transit or at rest). Additional direction is provided concerning security control of confidential information in transit. This provides an excellent reference for the regional compliance staff to assure security of data.

### **SERC's Portal**

SERC has an excellent web-based application used to collect information from its registered entities. This application provides the ability to easily obtain registrant information and quickly analyze compliance data. SERC was in the forefront of recognizing the need to develop a paperless reporting process. The reduction of hard copies adds to increased security of critical information. The portal system includes very robust controls in place for maintaining data security.

## Chapter 2 - Background

---

### Program Development

NERC compliance staff solicited proposals from four well-known, publicly recognized auditing firms. Three engagement types were provided by the auditing firms: 1) consultative; 2) management assertion; and 3) attestation of AUPs. NERC executive management and the compliance staff responsible for the project met on numerous occasions to discuss the options provided. An attestation of AUPs was determined the best vehicle to use for implementation of the NERC Regional Entity Audit Program as this type of engagement provides an audit format which is not open to subjectivity, and can be consistently applied.

Also, NERC contracted Crowe to develop a consulting report in the form of a management letter to identify any areas of process improvement noted during the development of the AUPs (management letter to NERC) and for each subsequent Regional Entity audit (management letter for each Regional Entity).

Jacqueline Power, a NERC Senior Regional Entity Compliance Program Auditor, worked with Crowe staff and the NERC program owners to develop the AUPs criteria. A listing of the AUPs references is captured in Appendix C.

Based on requests from the Regional Entities, NERC executive management determined to include other areas related to the Regional Entity's ERO functional requirements to the program during the first cycle of audits.<sup>4</sup> The decision was based on reducing the burden placed on the Regional Entities for supporting two separate audits. The Regional Reliability Standards Development Program, Funding, and Event Analysis were areas added to the Regional Entity Audit Program.

The Regional Entity's role in reliability assessments was not included in the audit activities as NERC maintains control of and plays an active role throughout this process. NERC's independent reliability assessment is based on constant communication with the eight regions regarding data collection, self-assessments, and development of reliability assessment reports. In addition, to address emerging reliability considerations, NERC obtains perspectives, data and information from the Regions to fortify its Special Reliability Assessments.

The draft AUPs were sent to each NERC program owner to review accuracy. NERC provided the draft AUPs to the eight Regional Entities and FERC for review and comment. This was done to promote and maintain transparency of the Regional Entity Audit Program. Based on comments received, NERC revised areas of the original audit plan, specifically in the area of funding and data security.

---

<sup>4</sup> See NERC Rules of Procedure at § 1207 ("Regional Entity Audits - Approximately every three years and more frequently if necessary for cause, NERC shall audit each regional entity to verify that the regional entity continues to comply with NERC rules of procedure and the obligations of NERC delegation agreement.").

## Chapter 3 – Audit Process

### **Compliance and Certification Committee Participation**

The CCC is a NERC BOT appointed stakeholder committee. The CCC monitors NERC's compliance with the RoP while maintaining independence of the execution of NERC's programs. In meeting its obligation, a CCC member was designated to observe the Regional Entity audit to maintain oversight of NERC's implementation of the Regional Entity Audit Program.

### **Pre-Audit**

Prior to the audit, NERC sent SERC three requests for information (RFI), Parts 1, 2 and 3, and corresponding questionnaires. RFI Part 1 focused on CMEP items; RFI Part 2 on the ERO functional responsibilities; and RFI Part 3 is specific to finance and budget. SERC responded and provided the requested information to NERC within the time specified.

NERC identified and provided to SERC each Crowe team member's work history, confidentiality agreements and conflict of interest statements. Also provided was the CCC member observing the audit, signed conflict of interest, confidentiality agreement statements and work history.

SERC designated a Compliance Auditor as the SPOC to coordinate audit information and requests. The SERC Compliance Auditor facilitated all audit activities between NERC and SERC's process owners. The SERC Compliance Auditor organized SERC's data and documentation on the secure Web site in a very concise format. This format was very beneficial for the audit team to quickly find the data needed to efficiently perform its audit objectives. NERC will use SERC's data filing matrix as an example for future Regional Entity audits.

### **Off-Site Audit Process**

The off-site week of the audit process was held at Crowe offices in Oakbrook, Illinois the week of June 1, 2009 and focused on SERC's processes and procedures. Interviews were not conducted with SERC staff for this week's audit activities. A NERC Senior Regional Entity Compliance Auditor was present to provide oversight, coordination and subject matter expertise to the Crowe staff. A staff member from FERC's OER was present as an observer of the process.

This was the first Regional Entity audit in which the use of an off-site week was incorporated. This approach proved to be very beneficial to the Crowe staff and improved the efficiency of the audit while on-site.

### Status Updates

A status update meeting was held with SERC at approximately 4:30 p.m. each day. Items discussed included:

- Completed activities for the day, including a dashboard of AUPs percentage completed;
- Planned activities for the following day;
- Interview schedules;
- Open requests for information items;
- Possible exceptions to the AUPs; and
- Possible management letter items.

SERC was provided the opportunity to comment to any potential exceptions items identified and supply additional evidence for clarification. By the end of the off-site week, the Crowe team completed the following percentages of the AUPs.

<b>AUP Number and Title</b>	<b>Completion</b>
II. Data Retention & Confidentiality	75%
III. Independence	50%
VIII. Compliance	85%
IX. Registrant Reporting	80%
X. Investigations	80%
XI. Notices	50%
XIII. Mitigation Plans	40%
XVI. ERO	50%

### On-Site Audit Process

The team arrived at SERC's offices on Monday, June 15, 2009 at 8:00 a.m. At 8:30 a.m., the President and CEO delivered a presentation containing an overview of SERC's organization to the audit team and observers. Key topics included:

- Background and history of SERC Reliability Corporation;
- Scope of SERC's footprint;
- Governance;
- Organization Chart;
- Summary of Compliance and Reliability Standards Activities; and
- Summary of other reliability service activities including technical committees, staff training, critical infrastructure protection, situational awareness, event analysis, alerts and recommendation tracking.

SERC's President and CEO highlighted SERC's organizational strengths. SERC's executive management's acknowledged the quality of its staff credentials and recognized the SERC staff for its efforts in supporting reliability.

SERC's relationship with its stakeholders for reliability improvement and strong technology focus via development and use of the secure portal was discussed.

SERC's Vice President and Director of Compliance delivered a presentation on SERC's compliance audit processes to the audit team. The scope of the audit program and SERC's emphasis on the on-site audits was discussed. SERC noted it performs greater than fifty audits per year. SERC assigns a staff person within its compliance audit group who is the subject matter expert and owner for each of the reliability standards. An overview of SERC's enforcement organization's processes and program scope was presented. This included in-depth discussion concerning processes for:

- Alleged Violation and Penalty Determination;
- Notices of Alleged Violation and Proposed Penalty or Sanction;
- Settlements Agreements; and
- Mitigation Plans.

SERC highlighted to date, greater than fifty percent of FERC-approved Notices of Penalty have been generated by SERC.

NERC delivered an overview of the NERC Regional Entity Audit Process to SERC. Topics included in the presentation were:

- Introductions of the audit team members and observers;
- Scope of the audit;
- Regional Entity audit regulatory references;
- Roles and responsibilities; and
- Deliverables and timelines.

Crowe and NERC staff held interviews with key SERC personnel to validate evidence presented. FERC staff and the CCC representative attended the majority of these interviews.

### **Status Updates**

At approximately 4:30 p.m. each day, a scheduled status update would occur with SERC executive and management personnel and the audit team. Items discussed were the same as previously mentioned in the off-site audit process of this report. SERC was provided the opportunity to discuss noted items and supply additional information for clarification.

### **Exit Presentation**

On June 19, 2009 at 3:30 p.m., NERC delivered an exit presentation to SERC. A Crowe executive discussed possible exceptions to the AUPs and management letter items. NERC provided results of the information systems assessment and the audit validation.

A scheduled week following the on-site audit was dedicated to Crowe performing further review of AUP potential exception items.

SERC was provided the opportunity to supply additional evidence up to Wednesday, June 24<sup>th</sup>, 2009. Crowe reviewed the additional evidence and made final determinations by the end of the week. The NERC audit of SERC was complete completed Friday, June 26, 2009.

### **Security and Confidentiality of Audit Evidence**

All information and data reviewed as part of the audit process is contained in electronic format. The electronic evidence was placed in a sealed, tamper-proof envelope verified by NERC staff and stored at a secure location. It will be retained for historical evidence per NERC's data retention policy.

## Chapter 4 – Financial and Budget Management

### Background

Pursuant to Section 8 (j), “Funding”<sup>5</sup> of the “Amended and Restated Regional Delegation Agreement between North American Electric Reliability Corporation and SERC Reliability Corporation,” NERC has the obligation to perform a review of SERC’s financial records at a minimum of every three years. NERC developed audit criteria with Crowe based on the requirements outlined in the delegation agreement and in the form of an agreed-upon procedure. The majority of criteria developed included items which an independent financial auditing firm should incorporate in its annual review of Regional Entities’ financial records. Based on subsequent discussions, it was determined that in lieu of duplicating the efforts of SERC’s independent auditing firm, SERC would provide NERC with copies of various requested documents. This would provide to NERC attestation that all items necessary for adherence to Section 8, were met and also provide NERC with an assurance concerning financial and budget items presented to the NERC BOT.

### Discussion of Review

NERC requested information in addition to SERC’s independent financial auditor report. NERC’s Chief Financial Officer performed a detailed review of the following documentation supplied by SERC:

1. Responses to the Pre-Audit Questionnaire;
2. Audit Arrangement letter from SERC’s independent financial auditing firm, dated December 31, 2008;
3. Form 990 Arrangement letter from SERC’s independent financial auditing firm, dated March 2, 2009;
4. Management Representation letter dated March 13, 2009;
5. Letter from SERC’s independent financial auditing firm, dated March 13, 2009 to the Board of Directors of SERC regarding auditor responsibility, scope and timing of the audit, accounting practices, etc.;
6. 2008 Quarterly Unaudited Financial Statements and Actual to Budget Variance Analysis;
7. 2008 Audited Financial Statements and Independent Auditor’s Report; and
8. 2009 Business Plan and Budget.

### Conclusion

SERC has complied with its obligations as required by its Regional Entity Delegation Agreement in Section 8, “Funding.” The Chief Financial Officer’s determination was based on the documentation provided including reliance upon the independent financial auditor’s report and the independent audit of the financial statements. No additional correspondence between SERC and its financial auditor was required.

---

<sup>5</sup> See the Executed “Amended and Restated Delegation Agreement between North American Electric Reliability Corporation and SERC Reliability Corporation,” at § 8(j) (“NERC shall have the right to review from time to time, in reasonable intervals but no less than every three years, the financial records of SERC in order to ensure that the documentation fairly represents in all material respects appropriate funding under this Agreement.”).

## Chapter 5 – Information Systems

---

### Discussion of Review

Pursuant to requirements outlined in RoP Section 402.3,<sup>6</sup> NERC staff in conjunction with Crowe staff developed criteria for assessing the Regional Entities' process for maintenance of data security, confidentiality and integrity.

NERC staff performed an assessment of SERC's processes for maintenance and control of its data security. This audit took place at SERC's offices in Charlotte from June 8, 2009 through June 11, 2009 and was performed by a NERC Senior Regional Entity Compliance Program Auditor and two Regional compliance auditors. Due to the confidential nature of the information reviewed, this report contains only a summary of key areas evaluated.

NERC staff identified four areas of improvement and made recommendations to SERC executive management during the exit presentation. NERC staff also identified one possible best practice associated with SERC's internal procedure titled "Staff Guide Data - Management and Confidentiality." Details of this procedure are found in the executive summary section, Chapter 1 of this report.

### Data Management, Security and Access Controls

The audit team reviewed SERC's data management procedures, which addressed data security, confidentiality, integrity, and retention requirements. These procedures addressed electronic and hard copy data supplied to SERC from its registered entities and internally created documents. NERC conducted multiple interviews with several SERC staff members that addressed treatment of different types a data, *i.e.*, physical or electronic data and the classification of data.

SERC places strict controls over its confidential data. The NERC audit team validated the controls by performing several tests to ensure unauthorized persons could not access the data. In addition, NERC performed spot checks of staff computers and verified SERC's adherence to security processes.

Per SERC's policy for access to electronic and physical data, only individuals with a business need are allowed access. SERC maintains an access list for both electronic and physical data. The audit team verified SERC followed its policy for removing access within the time specified for several employees who no longer worked for the SERC organization.

### Classification of Data

SERC provided sufficient documentation to describe its data classification procedure and treatment of sensitive data. SERC's procedures include guidance to its compliance staff on marking of physical and electronic documents and data to reflect sensitivity levels.

---

<sup>6</sup> See Rules of Procedure at § 402.3 ("Information Collection and Reporting — NERC and the regional entities shall implement data management procedures that address data reporting requirements, data integrity, data retention, data security, and data confidentiality.").

E-mails that include confidential information were appropriately labeled. The audit team selected several samples to verify consistent use of the classification and protection of confidential materials. The audit team concluded SERC adhered to its procedure for classifying data.

### **Data Transmittal**

SERC provided comprehensive documentation supporting its policies and procedures for transmitting and storing compliance data. The use of encryption, passwords, and other security measures are described in the documentation.

SERC provided a list of active employees who can transmit data related to the compliance and enforcement program both internally and externally. The audit team verified accuracy of the access list and subsequently used this list of employees to perform subsequent interviews to validate SERC's documented process was practiced. The audit team performed interviews and spot checks, and concluded SERC employees adhere to SERC's procedure for data transmittal.

### **Data Backup and Recovery**

SERC delegates backup data to an outside contractor for both its portal and SERC servers. SERC provided the executed contracts with its third-party vendors for the audit team's inspection. The audit team reviewed documentation, such as policies or procedures, that outlines how electronic information is stored externally (off-site) via a third-party vendor. SERC provided documentation of the third-party vendors' backup and recovery plan. Frequent backups of the data are performed and stored in two separate off-site facilities in a secure location. SERC provided evidence of system backups for a month, which was chosen by NERC staff. The audit team verified backups were performed per SERC's policy. The NERC audit team physically inspected one of the backup facilities.

### **Conclusion**

The audit team verified that SERC meets its responsibility as outlined in RoP Section 402.3. SERC has multiple processes and barriers in place for assuring and maintaining data integrity, data retention, data security, and data confidentiality.

## Chapter 6 – Compliance Audit Validation

---

### Discussion of Review

Pursuant of the RoP Section 402.1.3.2,<sup>7</sup> NERC, in maintaining its oversight of the Regional Entity Compliance Monitoring and Enforcement Program, is obligated to validate the results of a compliance audit performed by the Regional Entity on one of its registrants. To meet this obligation, NERC validated the results of an audit SERC previously performed on one of its registered entities. The audit team performing the validation included a Senior Regional Entity Compliance Program Auditor and a Regional compliance auditor. The NERC audit team reviewed the documentation supplied by the audited entity to SERC as evidence of compliance. The audit team performed a detailed review of the completed RSAWs and SERC'S audit report in making its determination.

The audited entity is registered as a Balancing Authority, Transmission Owner, Transmission Operator, Transmission Service Provider, Transmission Planner, Resource Planner, Planning Authority, Generator Owner, Load Serving Entity and Purchasing-Selling Entity. Previously, SERC's audit process was to perform two separate audits on a registered entity. One audit included operating standards while the other focused on the planning standards. The audit selected for NERC validation was performed by SERC under the previous auditing practice. Recently, SERC has changed this practice and performs an audit of all the applicable standards during one on-site visit. NERC validated the audit associated with the operating reliability standards. As such, the audit team performed an assessment of thirty-two reliability standards. The NERC Regional audit team verified that SERC included all reliability standards applicable to the audited entity. Detailed notes by the NERC Regional audit team were taken and recorded in the RSAWs submitted by SERC as evidence. These annotated RSAWs will be kept according to NERC's data retention policy as historical data.

### Conclusion

Upon review of the evidence presented, the NERC Regional audit team found the conclusions reached by SERC were accurate and supported by the evidence submitted to the Region by the registered entity.

---

<sup>7</sup> See Rules of Procedure at § 402.1.3.2 (“NERC shall establish a program to audit bulk power system owners, operators, and users operating within a regional entity to verify the findings of previous compliance audits conducted by the regional entity to evaluate how well the regional entity compliance enforcement program is meeting its delegated authority and responsibilities.”).

## Appendix A-AUP Exceptions to the Rules of Procedures, Delegation Agreement and Other

The exceptions listed in this Appendix A were quoted from the Crowe report. The notes were added by NERC for clarification.

### V – Reporting to NERC

*See* Crowe report at § V.D.8.c.i.a – (CMEP 6.5)

“Exception noted. For one (1) out of twelve (12) sampled registered entities (Sample No. 5 above), it was noted that SERC's transmittal of notification and Mitigation Plan to NERC did not occur within five (5) business days of the date SERC accepted the Mitigation Plan. Specifically, it was noted that SERC had accepted the Mitigation Plan on January 17, 2008, while the transmittal to NERC occurred on February 5, 2008 (after eleven (11) business days).”

### VIII – Compliance Activities

*See* Crowe report at § VIII.A.4.a.i – (RoP 403.7.5; CMEP 3.1.5; Compliance Auditor Manual, section 6)

“Exception noted. RoP 403.7.5 and CMEP 3.1.5 require that compliance audit participants complete required auditor training prior to the start of the audit. For one audit out of 5, one team member had not completed the required training courses before the start of the on-site audit. The audit was performed from 5/19/08 - 5/21/08. SERC indicated that the individual should have been listed as an observer instead of an audit team participant.”

*See* Crowe report at § VIII.A.4.n.ii.k.iii – (CMEP 3.1, Compliance Auditor Manual, section 12.2)

“Exception noted. CMEP 3.1 states, “All Compliance Audits shall be conducted in accordance with audit guides established for the Reliability Standards included in the compliance audit.” Section 12.3 of the Compliance Auditor Manual states that audit reports are to include information on supervisory reviews obtained. This is also included in the NERC audit report template. However, for 5 of 5 audits, the reports did not mention supervisory reviews.”

**Note:** During the interview process, SERC’s Manager of Audits stated he performed the supervisory review of each audit report but documentation of these supervisory reviews was not mentioned in the audit reports as required.

*See* Crowe report at § VIII.B.1.iii.b – (CMEP 3.3.1)

“Exception noted. According to CMEP 3.3.1, the RE is required to provide the registered entity the draft assessment and a chance for them to comment. For 5 out of 5 of the Spot Checks, the RE did not provide a draft assessment to the registered entity for them provide comments.”

## **XVI- ERO Functional Requirements**

*See Crowe report at § XVI.D.2.j – (Delegation Agreement – SERC’s Standard Development Process)*

“Exception noted. No documentation was provided to support that communication was sent to Regional Managers of the Regional Entities adjoining SERC (RFC, MRO, SPP, and FRCC) that the draft standard was posted for comment on SERC's website. In accordance with Exhibit C of the delegation agreement between SERC and NERC dated January 3, 2009 page 14, "A notice of the posting for a 30-day comment period will be sent to all SERC Standing Committees representatives and alternates. In addition, the notice will be sent (via e-mail) to NERC, the Regional Managers of the Regional Entities adjoining SERC (RFC, MRO, SPP, and FRCC)..."

Based on an inquiry with SERC management, subsequent to the development of the standards procedure, a regional reliability working group list was developed by NERC. This group includes the standards manager, but not the Region manager, for each neighboring region. This regional reliability working group was included on each communication sent by SERC for posting of the draft standard for comment.”

## Appendix B-AUP Exceptions

The exceptions listed in Appendix B were quoted from the Crowe report. The notes were added by NERC for clarification.

### III - Independence

**Note:** There are two distinct sections of Independence procedure which addresses governance and conflict of interest. One area is internal, *i.e.*, SERC staff and Board members, (Internal Regional Entity (RE) Governance and Conflict of Interest). The other area is relevant to personnel such as contractors (Conflict of Interest by External Parties). Due to this separation of application and although it pertains to the same criteria, it is noted as two exceptions.

#### **Internal Regional Entity (RE) Governance and Conflict of Interest**

*See* Crowe report at § III.A.4.a.iv.c

“Exception noted. Per inspection of SERC’s Conflict of Interest Policy dated December 3, 2008, the policy does not address a review of the COI statements.”

*See* Crowe report at § III.A.4.a.iiv.c

“Exception noted. Per inspection of SERC’s Conflict of Interest Policy dated December 3, 2008, the policy does not address a monitoring and enforcement of internal independence and conflict of interest policies.”

#### **Conflict of Interest by External Parties**

*See* Crowe report at § III.B.2.d.iii

“Exception noted. SERC’s policies do not address the review of conflict of interest statements.”

*See* Crowe report at § III.B.2.e.iii

“Exception noted. SERC’s policies do not address monitoring and enforcement of independence and conflict of interest policies.”

### VI - Registration

*See* Crowe report at § VI.A.12

“We selected 3 TOPs. Exceptions noted. The registration documentation provided for 3 of 3 TOPs we tested did not include verification that the entities met one of the criteria for registration as a TOP. Section III of NERC's Statement of Compliance Registry criteria states that TOs and TOPs should be excluded from registering under those functions if they do not meet one of the following criteria, and therefore, would be included in the registry if they do meet one of the criteria:

- \* Owning/operating an integrated transmission element associated with the bulk power system 100 kV and above, or lower voltage as defined by the RE necessary to provide for the reliable operation of the interconnected transmission grid; or

- \* Owning/operating a transmission element below 100 kV associated with a facility that is included on a critical facilities list.”

*See* Crowe report at § VI.B

“Exception noted. Although SERC's registration policy states, "NERC and SERC have the obligation to identify and register all entities that meet the criteria for inclusion in the Compliance Registry if the entity does not self register," SERC has no written procedures to assure that this is done. SERC did adopt written procedures for its initial efforts to register organizations that occurred from 2004 through 2007, but there is no going forward process for assuring that all required entities are registered. Since January 1, 2008, SERC identified 25 entities that were either not registered but should have been or were not registered for a function for which they should have been previously registered. The lack of a formal process for identifying potential registered entities increases the risk, that additional such organizations exist that have not been identified.”

**Note:** Similar to the note pertaining to Independence, the following three exceptions (V.C.1. b, c and d) are based on the same lack of documentation applied to different registration criteria and are located in separate steps within the Registration AUP.

*See* Crowe report at § VI.C.1.b

**Note:** VI.C.1.b pertains to verification that the relevant area was under only 1 RC.  
“Exceptions noted. SERC does not document this during the registration process.”

*See* Crowe report at § VI.C.1.c

**Note:** VI.C.1.c pertains to verification that each registered transmission element in its Region was under only 1 TP, PA, and TOP  
“Exceptions noted. SERC does not document this during the registration process.”

*See* Crowe report at § VI.C.1.d

**Note:** VI.C.1.d pertains to verification that checked each registered load and generator in their Region are only under 1 BA  
“Exceptions noted. SERC does not document this during the registration process.”

## **VIII – -Compliance**

*See* Crowe report at § VIII.A.4.i.ii.c

“Exception noted. For 3 of 5 compliance audits in our sample, not all checklist items on the RSAWs were marked complete. Specifically, RSAW checklists were not completed for 3 of 10 RSAWs we tested on one audit, 7 of 10 RSAWs we tested on another audit, and 5 of 10 RSAWs we tested on the third audit. Section 9.2 of the Compliance Auditor Manual, states that Regional Entities are to use the Reliability Standards Audit Worksheets (RSAWs) to document their review and assessment of compliance with reliability standards during compliance audits.”

## **XIII - Mitigation Plans**

*See* Crowe report at § XIII.A.2.a.i.a – (CMEP 6.4)

“Exception noted. According to the CMEP 6.4, the Mitigation Plan must be submitted within 30 days of the date of the NAVAPS. If the registered entity cannot submit the mitigation plan by the deadline, they must request an extension. Crowe noted in the AUP testing that 1 of 12 Mitigation Plans sampled was submitted after the 30 day window and no extension request was made.

During discussion with the Compliance Enforcement Manager, Crowe noted that this entity was supposed to have provided evidence of mitigation plan completion at the audit. The entity did not provide the information, so a NAVAPS was issued. It was also communicated to us that the entity submitted the mitigation plan late because they did not understand the process. The RE did not tell them to request the extension because they knew that the mitigating activities were completed and were in constant contact with the registered entity to get the plan submitted.

## Appendix C -AUP Procedures List

- I. Implementation Plan: (Section 4 CMEP, RoP 403.8, RoP 403.9, and RoP 403.21)
- II. Data Retention and Confidentiality: (Section 9 CMEP, RoP 402.8, RoP 403.6.4, RoP 403.7.4, RoP 403.14, RoP 403.16, RoP 408.3.1, RoP 502.2.1, and RoP 502.2.2)
- III. Independence [Organizational Independence and Conflict of Interest]: (RoP 402.8, RoP 403.1, RoP 403.6.1, RoP 403.6.2, RoP 403.6.3, RoP 403.6.5, RoP 403.7.1, RoP 403.7.2, and RoP 403.7.3)
- IV. Information Systems: (RoP 402.3)
- V. Reporting to NERC: (Section 8 CMEP, RoP 401.3, RoP 403.10 , RoP 403.15, RoP 403.19, RoP 403.20, RoP 403.21.1, RoP 408.1, RoP 408.2, RoP 408.4, RoP 410.3, RoP 502.1.4, RoP 502.1.5, RoP 503.3.3.3, RoP 503.3.3.4, RoP 504.2, RoP 507.4, RoP 507.6, and throughout the CMEP sections)
- VI. Registration: (Section 2 CMEP, RoP 500, Appendix 5)
- VII. Certification: (Section 2 CMEP, RoP 500, Appendix 5)
- VIII. Compliance (Audits and Spot Checks): (Section 3.1 CMEP, RoP 403.7.5, & RoP 403.11; Section 3.3 CMEP, and RoP 403.10.6)
- IX. Registered Entity Reporting (Self-Certifications, Exception Reporting, Self-Reporting, Periodic Data Submittals): (Section 3.2 CMEP, Section 3.7 CMEP, Section 3.5 CMEP, Section 3.6)
- X. Investigations (Compliance Violation Investigations, Complaints): Section 3.4 CMEP, and RoP 403.13, (Section 3.8 CMEP)
- XI. Notices (Possible, Alleged and Notices of Confirmed or Dismissals): (Section 5.1 CMEP)
- XII. Penalties and Sanctions: (RoP 403.17, RoP 407.2, and Appendix 4B)
- XIII. Mitigation plans: (RoP 403.18, and Section 6 CMEP)
- XIV. Remedial actions: (Section 7 CMEP)
- XV. Hearings (Attachment 2 of the CMEP): (RoP 403.4, RoP 403.20, and RoP 407.3)
- XVI. ERO Functional Requirements (Delegation Agreements)
  - a. Finance and Budget Management
  - b. Event Analysis
  - c. Regional Reliability Standards Development Program