



# **Compliance Audit Report Public Version**

**South Carolina Public Service Authority  
NCR01312  
October 19-22, 2009**

**Confidential Information (including  
Privileged and Critical Energy Infrastructure  
Information) – Has Been Removed**

**February 23, 2010**

## TABLE OF CONTENTS

Executive Summary .....	3
Audit Process .....	3
<i>Objectives</i> .....	4
<i>Scope</i> .....	4
<i>Confidentiality and Conflict of Interest</i> .....	4
<i>On-site Audit</i> .....	4
<i>Methodology</i> .....	5
<i>Audit Overview</i> .....	5
<i>Audit</i> .....	5
<i>Exit Briefing</i> .....	6
<i>Company Profile</i> .....	6
<i>Audit Specifics</i> .....	6
Audit Results.....	7
<i>Findings</i> .....	8
<i>Compliance Culture</i> .....	18

## EXECUTIVE SUMMARY

South Carolina Public Service Authority (SCPSA) was audited on October 19-22, 2009 for compliance with the requirements contained in the currently mandatory and enforceable reliability standards in the 2009 NERC Compliance Monitoring and Enforcement Program (CMEP) that are applicable to SCPSA's registered functions. SCPSA is registered with SERC Reliability Corporation (SERC) as a Balancing Authority (BA), Distribution Provider (DP), Generator Operator (GOP), Generator Owner (GO), Interchange Authority (IA), Load-Serving Entity (LSE), Planning Authority (PA), Purchasing-Selling Entity (PSE), Resource Planner (RP), Transmission Owner (TO), Transmission Planner (TP), Transmission Operator (TOP), and Transmission Service Provider (TSP). Thirty-nine standards were selected and identified to SCPSA as subject to review during this audit. The audit focused on documents and other evidence provided to SERC by the staff of SCPSA, and did not include any evidence obtained through system observation or inspection. The findings of the audit are based on the state of compliance and current mitigation activity at the time of the audit, and do not reflect past compliance activities or activities that will be completed in the future. A spot check of the 13 CIP requirements that SCPSA was required to be compliant with as of July 1, 2008 was conducted, however the details of the spot check will be covered in a separate written report.

SCPSA staff was requested to provide valid evidence of meeting each and every applicable requirement and sub-requirement contained in each standard that had been previously identified by SERC Compliance staff to SCPSA as subject to this audit. SCPSA staff responded by providing evidence in the form of reports, procedures, studies, and other documents. SCPSA staff then cited specific portions of the evidence that demonstrated compliance. This evidence and the citations were documented and evaluated by the audit team to assess the level of compliance. If all of the requirements and sub-requirements of an audited standard were met, then SCPSA was judged to be compliant. Likewise, if any of the requirements or sub-requirements were not fully met, then SCPSA was judged to have a possible violation of the standard. A score of 100% is required for compliance.

SCPSA was found to be in compliance with all but three of the standards that were audited. The audit team determined that SCPSA had possible violations of NERC Reliability Standards including: FAC-008-1 R1, FAC-009-1 R1, and PRC-005-1 R1 and R2.

This audit report includes information about how far SCPSA missed the requirements for the possible compliance violations. This information will be used to help determine the severity level of sanctions and penalties. The possible compliance violations will be processed through the SERC CMEP. Any further actions related to possible compliance violations will be through that process.

The link to the South Carolina Public Service Authority NOP can be viewed [here](#).

## AUDIT PROCESS

The compliance audit process steps are detailed in the NERC CMEP. The NERC CMEP generally conforms to the United States Government Accountability Office Government Auditing Standards and other generally accepted audit practices.

### **Objectives**

All registered entities are subject to audit for compliance with all reliability standards applicable to the functions for which the registered entity is registered.<sup>1</sup> The audit objectives are:

- Independently review SCPSA's compliance with the requirements of the reliability standards that are applicable to SCPSA based on the SCPSA registered functions.
- Validate compliance with applicable reliability standards from the NERC 2009 Implementation Plan list of actively monitored standards.
- Validate evidence of self-reported violations and previous self-certifications, confirm compliance with other requirements of the reliability standard, and review the status of associated mitigation plans.
- Document SCPSA's compliance culture.

### **Scope**

The scope of the audit of SCPSA included all monitored standards that are in the NERC 2009 CMEP. Based on the confirmed registration of SCPSA, the thirty-nine reliability standards previously identified were the focus of the compliance audit.

Note: For the 2009 compliance program, the monitoring period for the compliance audit will generally be the lesser of: 1) Date of registration to current date; 2) Date of last audit or spot check to current date; or, 3) June 18, 2007 to current date. The monitoring period is not limited to the time period for which penalties and sanctions are assessed.

### **Confidentiality and Conflict of Interest**

Code of conduct documentation for the regional entity staff were provided to SCPSA in advance of the audit. Work history and conflict of interest forms submitted by each audit team member were provided to SCPSA upon request. SERC has confirmed that confidentiality agreements have been executed by, and are on file for SERC Industry Subject Matter Experts (SMEs) who participated in the audit. SCPSA was given an opportunity to object to an audit team member on the basis of a possible conflict of interest or the existence of other circumstances that could interfere with the audit team member's impartial performance of duties. SCPSA accepted the audit team member participants with no objections.

### **On-site Audit**

SCPSA was contacted by letter on April 24, 2009 by SERC staff. The letter provided SCPSA with their initial notification of their upcoming audit in 2009, and the desire to schedule audit dates that would be acceptable to both parties. SERC staff then provided formal acknowledgement of the scheduled audit dates and requested that SCPSA both verify their currently registered functions and complete and return an attached Pre-Audit Survey within 30 days.

On July 22, 2009, SERC staff forwarded an Audit Detail Letter to SCPSA, again confirming the scheduled audit dates and confirming SCPSA's registered functions within SERC. The Audit Detail Letter also provided SCPSA with notice of the Standards in Audit Scope, Proposed Audit Schedule, Audit Team Roster (with industry affiliations), and requested that SCPSA SMEs responsible for and knowledgeable of compliance submittals be available for interview during the audit. In addition to the Audit Detail Letter, SCPSA was provided with a Non-Disclosure Agreement Signature Verification for audit team members, a list of Documentation and

---

<sup>1</sup> North American Electric Reliability Corporation CMEP, paragraph 3.1, Compliance Audits

Evidence Requirements, and Questionnaire and Reliability Standard Auditor Worksheets (QRSAWs) for each standard to be audited.

Interviews with SMEs were requested, in conjunction with documented evidence, to provide the audit team with additional information or clarification as a basis for professional judgment when validating compliance with reliability standards.

### ***Methodology***

A team of auditors and Industry SMEs were identified and conducted the audit of SCPSA. The standards were grouped and scheduled for review to make the most efficient use of SCPSA staff's time. The Audit Team Leader (ATL), or his designee, initiated dialogue on each standard requirement and requested compliance evidence. This evidence, and SCPSA's staff responses, was documented. SCPSA staff was requested to show valid evidence of meeting each applicable requirement and sub-requirement contained in the thirty-nine standards that had been previously identified by SERC to SCPSA as subject to this audit. SCPSA staff responded by providing evidence in the form of reports, procedures, studies, and other documents. SCPSA staff would then cite specific portions of the evidence that demonstrated compliance.

This evidence and the citations were documented by the audit team scribe on the QRSAWs, and were evaluated by the audit team for the level of compliance and agreement with the requirement. Discrepancies between the requirement and the evidence provided were the subject of dialogue among the team members and SCPSA staff members until it was determined whether each requirement was met by the evidence offered.

Once all the evidence was presented and discussed, if SCPSA did not provide sufficient evidence to support a finding of compliance, then a possible violation would have been identified by the team, and SCPSA staff would have been informed.

### ***Audit Overview***

The audit team arrived at the SCPSA offices at 3:00 PM, October 19, 2009. At 4:00 PM a SERC Senior Compliance Auditor, began the session with an opening presentation. He reviewed the NERC compliance plan for 2009 in general, and how it applied to SCPSA specifically. He introduced and reviewed the standards to be covered in the audit, and addressed both the expectations of SCPSA staff and the quality of evidence to be presented. The opening presentation also covered the basic procedures for the audit, and the bounding rules of conduct. SCPSA staff made a brief presentation describing SCPSA's corporate structure and compliance program. The staff of SCPSA was introduced, and general housekeeping matters explained. The SCPSA staff provided a tour of the Operations Control room. The staff of SCPSA was excused and the audit team reviewed team assignments and a general overview for preparation of the audit activities. The audit team left the SCPSA office at 6:04 PM, October 19, 2009 to return the next day to start the review of the reliability standards in the audit scope.

### ***Audit***

The audit team arrived at the SCPSA office at 7:45 AM, October 20, 2009. The audit team was divided into two sub-teams. The audit team initially reviewed the registration status of SCPSA with entity staff to verify applicability of each standard. Each standard's audit began with a recitation of each requirement. SCPSA staff then presented evidence supporting requirement compliance, or cited evidence previously provided to the audit team. At that point, the evidence was reviewed and discussed until the team reached agreement on the evidence. By audit team consensus, a determination of compliance was reached for each of the requirements and communicated to SCPSA staff before proceeding to the next requirement. At that point the team

scribe would record the evidence presented to satisfy the requirement, and the team's recommendation on that requirement, using the QRSAs.  
The review of all applicable standards was completed at 1:50 PM, October 22, 2009 and the audit team met to review and discuss the findings. Following these discussions, the scribe collected all notes and evidence as needed and began to finalize the QRSAs.

### ***Exit Briefing***

A SERC Senior Compliance Auditor and the Audit Team Leader (ATL) presented an exit briefing to the assembled audit team and entity staff at 2:35 PM, October 22, 2009. This was followed by an informal response and questions from the SCPSA staff. The exit briefing summarized the team's preliminary conclusions, including any items of potential noncompliance or possible violation with supporting information, areas of concern, any added information required and the expected timeline for review and issuance of the audit report.

The ATL solicited both informal comments from SCPSA staff, along with requesting that they fill out formal feedback forms for submission to NERC and SERC.

The ATL thanked SCPSA staff for their cooperation and support of the audit process. SCPSA staff expressed their appreciation of the professional manner in which the audit was conducted.

The audit team left the SCPSA meeting room at 3:20 PM on October 22, 2009.

### ***Company Profile***

South Carolina Public Service Authority (also known as Santee Cooper) is South Carolina's state-owned electric and water utility. As the state's largest power producer, SCPSA, along with 20 electric cooperatives, generates and/or supplies electricity to approximately two million South Carolinians in all 46 of the state's counties.

### ***Audit Specifics***

The compliance audit was conducted during October 19–22, 2009 at the SCPSA office in Moncks Corner, SC.

### **Audit Team**

<b>Audit Team Role</b>	<b>Title</b>	<b>Company</b>
Audit Team Lead	Senior Compliance Auditor	SERC
Member	Senior Compliance Auditor	SERC
Member	Senior Compliance Auditor	SERC
Member	Senior Compliance Auditor	SERC
Member	Compliance Auditor	SERC
Member	ISME	SIPC
Member	ISME	Midwest ISO
Member	ISME	TVA
Member	ISME	EKPC

### **SCPSA Audit Participants**

Sr. VP, Power Delivery	SCPSA
Vice President, Planning and Power Supply	SCPSA
Supervisor, System Control	SCPSA

Supervisor, System SCADA	SCPSA
Superintendent, Operations	SCPSA
Principal Engineer, Generation	SCPSA
Deputy Chief, Law Enforcement and Security	SCPSA
Supervisor, Power Supply Planning	SCPSA
Principal Engineer, System Control	SCPSA
Principal Engineer, System Control	SCPSA
General Supervisor, Transmission Planning	SCPSA
Supervisor, Support & Special Studies	SCPSA
Manager, Transmission Operations	SCPSA
Superintendent, Right-of-Way Management	SCPSA
Supervisor, Transmission Studies	SCPSA
Manager, Transmission Technical	SCPSA
Superintendent, System Protection and Control	SCPSA
Supervisor, System Protection and Control	SCPSA
Superintendent, Maintenance , Generation	SCPSA
Superintendent, Operations, Generation	SCPSA

## AUDIT RESULTS

The audit team reviewed documents provided by SCPSA prior to the audit, as requested in the Documentation and Evidence Requirements section of SCPSA's Compliance Audit Certification Letter. A pre-audit review of these documents and any currently open or recently closed mitigation plans helped to establish the audit team's focus during the audit.

The audit team reviewed the evidence provided by SCPSA to substantiate compliance with each standard requirement. The team requested clarification and/or additional supporting and corroborating evidence, as required, to obtain sufficient and appropriate evidence to support a determination of compliance.

In instances where the evidence provided by SCPSA represented multiple facilities and/or large quantities of equipment, the audit team haphazardly selected evidence samples, from the different facilities and/or equipment, to facilitate a consensus agreement of the team whether SCPSA was, in the team's professional judgment, satisfactorily meeting the requirements of the standard or is in possible violation of the requirement.

The audit team reviewed SCPSA's status and progress of mitigation of all open and/or recently closed mitigation plans in conjunction with the review of each standard applicable to SCPSA's currently registered functions.

If the audit team determined that the evidence provided by SCPSA was insufficient or inappropriate to substantiate a determination of compliance, the team immediately informed SCPSA's Subject Matter Expert(s) of this fact. Additionally, the Audit Team Leader, through coordination with SCPSA's audit coordinators, ensured that SCPSA's management was made aware of the potential for a finding of a possible violation in each instance, and of the basis for the team's determination.

The Audit Team Leader clearly identified the team’s findings of compliance and basis for their findings, areas of concern, and available remedies in an exit presentation to SCPSA’s management upon completion of the audit.

The audit team documented their review and determination of compliance of each standard requirement on Questionnaire/Reliability Standard Auditor Worksheets. SCPSA’s policies, procedures, screenshots, operator logs, audio clips, correspondence and other evidence presented, as well as auditor comments and determinations of compliance documented on the QRSAs, were used in formulating this report.

The audit team determined that SCPSA had possible violations of NERC Reliability Standards, including: FAC-008-1 R1, FAC-009-1 R1, and PRC-005-1 R1 and R2.

Prior to being forwarded to SERC’s Manager of Compliance Audits, or his designee, for review and approval as SERC’s Final Confidential Non-Public Audit Report of SCPSA, the content and accuracy of this report:

- Is reviewed and commented on by all audit team members
- Is reviewed by SCPSA’s management for correction and comment, and
- Is reviewed and approved by the Audit Team Leader.

Upon final disposition of any possible violations determined by the audit team, if any, and redaction of appropriate information contained herein, this report will be reviewed and approved by SERC’s Vice President and Director of Compliance before being issued as SERC’s Final Public Audit Report of SCPSA.

### ***Findings***

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
BAL-001-0a	R1.	N/A
BAL-001-0a	R2.	N/A
BAL-001-0a	R3.	N/A
BAL-001-0a	R4.	N/A
BAL-002-0	R1.	Compliant
BAL-002-0	R2.	Compliant
BAL-002-0	R3.	Compliant
BAL-002-0	R4.	N/A
BAL-002-0	R5.	N/A
BAL-002-0	R6.	N/A
BAL-003-0a	R1.	N/A
BAL-003-0a	R2.	N/A
BAL-003-0a	R3.	N/A
BAL-003-0a	R4.	N/A
BAL-003-0a	R5.	N/A
BAL-003-0a	R6.	N/A
BAL-004-0	R1.	N/A
BAL-004-0	R2.	N/A
BAL-004-0	R3.	N/A
BAL-004-0	R4.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
BAL-005-0b	R1.	N/A
BAL-005-0b	R2.	Compliant
BAL-005-0b	R3.	N/A
BAL-005-0b	R4.	N/A
BAL-005-0b	R5.	N/A
BAL-005-0b	R6.	N/A
BAL-005-0b	R7.	N/A
BAL-005-0b	R8.	N/A
BAL-005-0b	R9.	N/A
BAL-005-0b	R10.	Compliant
BAL-005-0b	R11.	N/A
BAL-005-0b	R12.	N/A
BAL-005-0b	R13.	N/A
BAL-005-0b	R14.	N/A
BAL-005-0b	R15.	N/A
BAL-005-0b	R16.	N/A
BAL-005-0b	R17.	N/A
BAL-006-1	R1.	N/A
BAL-006-1	R2.	N/A
BAL-006-1	R3.	N/A
BAL-006-1	R4.	N/A
BAL-006-1	R5.	N/A
CIP-001-1	R1.	Compliant
CIP-001-1	R2.	Compliant
CIP-001-1	R3.	Compliant
CIP-001-1	R4.	Compliant
CIP-002-1 through CIP-009-1		N/A
COM-001-1	R1.	Compliant
COM-001-1	R2.	N/A
COM-001-1	R3.	N/A
COM-001-1	R4.	N/A
COM-001-1	R5.	N/A
COM-001-1	R6.	N/A
COM-002-2	R1.	Compliant
COM-002-2	R2.	N/A
EOP-001-0	R1.	Compliant
EOP-001-0	R2.	Compliant
EOP-001-0	R3.	Compliant
EOP-001-0	R4.	Compliant
EOP-001-0	R5.	Compliant
EOP-001-0	R6.	Compliant
EOP-001-0	R7.	Compliant

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
EOP-002-2	R1.	Compliant
EOP-002-2	R2.	Compliant
EOP-002-2	R3.	Compliant
EOP-002-2	R4.	Compliant
EOP-002-2	R5.	Compliant
EOP-002-2	R6.	Compliant
EOP-002-2	R7.	Compliant
EOP-002-2	R8.	N/A
EOP-002-2	R9.	Compliant
EOP-003-1	R1.	Compliant
EOP-003-1	R2.	Compliant
EOP-003-1	R3.	Compliant
EOP-003-1	R4.	Compliant
EOP-003-1	R5.	Compliant
EOP-003-1	R6.	Compliant
EOP-003-1	R7.	Compliant
EOP-003-1	R8.	Compliant
EOP-004-1	R1.	N/A
EOP-004-1	R2.	N/A
EOP-004-1	R3.	N/A
EOP-004-1	R4.	N/A
EOP-004-1	R5.	N/A
EOP-005-1	R1.	Compliant
EOP-005-1	R2.	Compliant
EOP-005-1	R3.	Compliant
EOP-005-1	R4.	Compliant
EOP-005-1	R5.	Compliant
EOP-005-1	R6.	Compliant
EOP-005-1	R7.	Compliant
EOP-005-1	R8.	Compliant
EOP-005-1	R9.	Compliant
EOP-005-1	R10.	Compliant
EOP-005-1	R11.	Compliant
EOP-006-1	R1.	N/A
EOP-006-1	R2.	N/A
EOP-006-1	R3.	N/A
EOP-006-1	R4.	N/A
EOP-006-1	R5.	N/A
EOP-006-1	R6.	N/A
EOP-008-0	R1.	Compliant
EOP-009-0	R1.	N/A
EOP-009-0	R2.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
FAC-001-0	R1.	Compliant
FAC-001-0	R2.	Compliant
FAC-001-0	R3.	Compliant
FAC-002-0	R1.	N/A
FAC-002-0	R2.	N/A
FAC-003-1	R1.	Compliant
FAC-003-1	R2.	Compliant
FAC-003-1	R3.	N/A
FAC-003-1	R4.	N/A
FAC-008-1	R1.	Possible Violation
FAC-008-1	R2.	Compliant
FAC-008-1	R3.	Compliant
FAC-009-1	R1.	Possible Violation
FAC-009-1	R2.	Compliant
FAC-010-1	R1.	N/A
FAC-010-1	R2.	Compliant
FAC-010-1	R3.	N/A
FAC-010-1	R4.	N/A
FAC-010-1	R5.	N/A
FAC-011-1	R1.	N/A
FAC-011-1	R2.	N/A
FAC-011-1	R3.	N/A
FAC-011-1	R4.	N/A
FAC-011-1	R5.	N/A
FAC-013-1	R1.	N/A
FAC-013-1	R2.	N/A
FAC-014-1	R1.	N/A
FAC-014-1	R2.	N/A
FAC-014-1	R3.	N/A
FAC-014-1	R4.	N/A
FAC-014-1	R5.	Compliant
FAC-014-1	R6.	N/A
INT-001-3	R1.	N/A
INT-001-3	R2.	N/A
INT-003-2	R1.	N/A
INT-004-2	R1.	N/A
INT-004-2	R2.	N/A
INT-005-2	R1.	N/A
INT-006-2	R1.	N/A
INT-007-1	R1.	N/A
INT-008-2	R1.	N/A
INT-009-1	R1.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
INT-010-1	R1.	N/A
INT-010-1	R2.	N/A
INT-010-1	R3.	N/A
IRO-001-1	R1.	N/A
IRO-001-1	R2.	N/A
IRO-001-1	R3.	N/A
IRO-001-1	R4.	N/A
IRO-001-1	R5.	N/A
IRO-001-1	R6.	N/A
IRO-001-1	R7.	N/A
IRO-001-1	R8.	Compliant
IRO-001-1	R9.	N/A
IRO-002-1	R1.	N/A
IRO-002-1	R2.	N/A
IRO-002-1	R3.	N/A
IRO-002-1	R4.	N/A
IRO-002-1	R5.	N/A
IRO-002-1	R6.	N/A
IRO-002-1	R7.	N/A
IRO-002-1	R8.	N/A
IRO-002-1	R9.	N/A
IRO-003-2	R1.	N/A
IRO-003-2	R2.	N/A
IRO-004-1	R1.	N/A
IRO-004-1	R2.	N/A
IRO-004-1	R3.	Compliant
IRO-004-1	R4.	Compliant
IRO-004-1	R5.	N/A
IRO-004-1	R6.	N/A
IRO-004-1	R7.	Compliant
IRO-005-1	R1.	N/A
IRO-005-1	R2.	N/A
IRO-005-1	R3.	N/A
IRO-005-1	R4.	N/A
IRO-005-1	R5.	N/A
IRO-005-1	R6.	N/A
IRO-005-1	R7.	N/A
IRO-005-1	R8.	Compliant
IRO-005-1	R9.	N/A
IRO-005-1	R10.	N/A
IRO-005-1	R11.	N/A
IRO-005-1	R12.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
IRO-005-1	R13.	Compliant
IRO-005-1	R14.	N/A
IRO-005-1	R15.	N/A
IRO-005-1	R16.	N/A
IRO-005-1	R17.	N/A
IRO-006-3	R1.	N/A
IRO-006-3	R2.	N/A
IRO-006-3	R3.	N/A
IRO-006-3	R4.	N/A
IRO-006-3	R5.	N/A
IRO-006-3	R6.	Compliant
IRO-014-1	R1.	N/A
IRO-014-1	R2.	N/A
IRO-014-1	R3.	N/A
IRO-014-1	R4.	N/A
IRO-015-1	R1.	N/A
IRO-015-1	R2.	N/A
IRO-015-1	R3.	N/A
IRO-016-1	R1.	N/A
IRO-016-1	R2.	N/A
MOD-006-0	R1.	N/A
MOD-006-0	R2.	N/A
MOD-007-0	R1.	N/A
MOD-007-0	R2.	N/A
MOD-010-0	R1.	N/A
MOD-010-0	R2.	N/A
MOD-012-0	R1.	N/A
MOD-012-0	R2.	N/A
MOD-016-1	R1.	N/A
MOD-016-1	R2.	N/A
MOD-016-1	R3.	N/A
MOD-017-0	R1.	N/A
MOD-018-0	R1.	N/A
MOD-018-0	R2.	N/A
MOD-019-0	R1.	N/A
MOD-020-0	R1.	N/A
MOD-021-0	R1.	N/A
MOD-021-0	R2.	N/A
MOD-021-0	R3.	N/A
NUC-001-1	R1.	N/A
NUC-001-1	R2.	N/A
NUC-001-1	R3.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
NUC-001-1	R4.	N/A
NUC-001-1	R5.	N/A
NUC-001-1	R6.	N/A
NUC-001-1	R7.	N/A
NUC-001-1	R8.	N/A
NUC-001-1	R9.	N/A
PER-001-0	R1.	Compliant
PER-002-0	R1.	Compliant
PER-002-0	R2.	Compliant
PER-002-0	R3.	Compliant
PER-002-0	R4.	Compliant
PER-003-0	R1.	Compliant
PER-004-1	R1.	N/A
PER-004-1	R2.	N/A
PER-004-1	R3.	N/A
PER-004-1	R4.	N/A
PER-004-1	R5.	N/A
PRC-001-1	R1.	Compliant
PRC-001-1	R2.	Compliant
PRC-001-1	R3.	Compliant
PRC-001-1	R4.	Compliant
PRC-001-1	R5.	Compliant
PRC-001-1	R6.	N/A
PRC-004-1	R1.	Compliant
PRC-004-1	R2.	Compliant
PRC-004-1	R3.	Compliant
PRC-005-1	R1.	Possible Violation
PRC-005-1	R2.	Possible Violation
PRC-007-0	R1.	N/A
PRC-007-0	R2.	N/A
PRC-007-0	R3.	N/A
PRC-008-0	R1.	Compliant
PRC-008-0	R2.	Compliant
PRC-009-0	R1.	N/A
PRC-009-0	R2.	N/A
PRC-010-0	R1.	N/A
PRC-010-0	R2.	N/A
PRC-011-0	R1.	N/A
PRC-011-0	R2.	N/A
PRC-015-0	R1.	N/A
PRC-015-0	R2.	N/A
PRC-015-0	R3.	N/A

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
PRC-016-0	R1.	N/A
PRC-016-0	R2.	N/A
PRC-016-0	R3.	N/A
PRC-017-0	R1.	N/A
PRC-017-0	R2.	N/A
PRC-018-1	R1.	N/A
PRC-018-1	R2.	N/A
PRC-018-1	R3.	N/A
PRC-018-1	R4.	N/A
PRC-018-1	R5.	N/A
PRC-018-1	R6.	N/A
PRC-021-1	R1.	N/A
PRC-021-1	R2.	N/A
PRC-022-1	R1.	N/A
PRC-022-1	R2.	N/A
TOP-001-1	R1.	Compliant
TOP-001-1	R2.	Compliant
TOP-001-1	R3.	Compliant
TOP-001-1	R4.	Compliant
TOP-001-1	R5.	Compliant
TOP-001-1	R6.	Compliant
TOP-001-1	R7.	Compliant
TOP-001-1	R8.	Compliant
TOP-002-2	R1.	Compliant
TOP-002-2	R2.	N/A
TOP-002-2	R3.	Compliant
TOP-002-2	R4.	Compliant
TOP-002-2	R5.	N/A
TOP-002-2	R6.	N/A
TOP-002-2	R7.	N/A
TOP-002-2	R8.	N/A
TOP-002-2	R9.	Compliant
TOP-002-2	R10.	N/A
TOP-002-2	R11.	Compliant
TOP-002-2	R12.	N/A
TOP-002-2	R13.	Compliant
TOP-002-2	R14.	Compliant
TOP-002-2	R15.	Compliant
TOP-002-2	R16.	Compliant
TOP-002-2	R17.	Compliant
TOP-002-2	R18.	Compliant
TOP-002-2	R19.	Compliant

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
TOP-003-0	R1.	Compliant
TOP-003-0	R2.	Compliant
TOP-003-0	R3.	Compliant
TOP-003-0	R4.	N/A
TOP-004-1	R1.	Compliant
TOP-004-1	R2.	Compliant
TOP-004-1	R3.	Compliant
TOP-004-1	R4.	Compliant
TOP-004-1	R5.	Compliant
TOP-004-1	R6.	N/A
TOP-005-1	R1.	N/A
TOP-005-1	R2.	N/A
TOP-005-1	R3.	N/A
TOP-005-1	R4.	N/A
TOP-006-1	R1.	N/A
TOP-006-1	R2.	Compliant
TOP-006-1	R3.	N/A
TOP-006-1	R4.	N/A
TOP-006-1	R5.	N/A
TOP-006-1	R6.	Compliant
TOP-006-1	R7.	Compliant
TOP-007-0	R1.	Compliant
TOP-007-0	R2.	Compliant
TOP-007-0	R3.	Compliant
TOP-007-0	R4.	N/A
TOP-008-1	R1.	Compliant
TOP-008-1	R2.	Compliant
TOP-008-1	R3.	Compliant
TOP-008-1	R4.	N/A
TPL-001-0	R1.	Compliant
TPL-001-0	R2.	N/A
TPL-001-0	R3.	N/A
TPL-002-0	R1.	Compliant
TPL-002-0	R2.	N/A
TPL-002-0	R3.	N/A
TPL-003-0	R1.	Compliant
TPL-003-0	R2.	N/A
TPL-003-0	R3.	N/A
TPL-004-0	R1.	N/A
TPL-004-0	R2.	N/A
VAR-001-1	R1.	Compliant
VAR-001-1	R2.	Compliant

Confidential Information (including Privileged and  
Critical Energy Infrastructure Information) – Has Been Removed

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
VAR-001-1	R3.	N/A
VAR-001-1	R4.	N/A
VAR-001-1	R5.	Compliant
VAR-001-1	R6.	N/A
VAR-001-1	R7.	Compliant
VAR-001-1	R8.	Compliant
VAR-001-1	R9.	Compliant
VAR-001-1	R10.	Compliant
VAR-001-1	R11.	N/A
VAR-001-1	R12.	Compliant
VAR-002-1	R1.	N/A
VAR-002-1	R2.	N/A
VAR-002-1	R3.	N/A
VAR-002-1	R4.	N/A
VAR-002-1	R5.	N/A

### **Compliance Culture**

The audit team assessed SCPSA's Internal Compliance Program in conjunction with the audit. Evidence reviewed in assessing the program included: SCPSA's Compliance Pre-Audit Survey, SCPSA Reliability Standards Compliance Program document, compliance staff organizational charts, interviews with SCPSA staff, and observation of staff responses in preparation for and during the audit.

Four factors that characterize a vigorous and effective compliance program are: active engagement and leadership by a company's senior management; preventive measures appropriate to the individual circumstances of the company; promptly detecting, stopping, and reporting a violation; and, ultimately fixing the problem and working to avoid future possible violations.

SERC recognizes that there isn't one standard formula for an effective compliance program, and that there will be variations in each company's program and culture based on countless factors, including the size and age of the company, as well as the nature and extent of its business. Ultimately what matters are the results, and whether the compliance program worked as it should.

The audit team determined that SCPSA's Internal Compliance Program documents and their staff's demonstrated compliance culture indicate an effective compliance program.