



Compliance Audit Report Public

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

**Sacramento Municipal Utility District
(SMUD)**

December 10 – 14, 2007

April 20, 2010

TABLE OF CONTENTS

Executive Summary	3
Audit Process	4
<i>Objectives</i>	4
<i>Scope</i>	5
<i>Confidentiality and Conflict of Interest</i>	5
<i>On-site Audit</i>	5
<i>Methodology</i>	6
<i>Audit Overview</i>	6
<i>Audit</i>	7
<i>Exit Briefing</i>	8
<i>Company Profile</i>	8
<i>Audit Specifics</i>	9
Audit Results	11
<i>Findings</i>	12
<i>Compliance Culture</i>	21

EXECUTIVE SUMMARY

Note - This compliance audit report provides a record of SMUD's compliance status as documented by the WECC Compliance Department during the on-site audit of December 10-14, 2007. This report does not reflect any actions SMUD may have taken since the on-site audit.

The WECC Compliance Department conducted an On-site Compliance Audit of the Sacramento Municipal Utility District (SMUD) on December 10 through 14, 2007. The audit was conducted at the SMUD Headquarters in Sacramento, California. The Audit Team was made up of WECC Compliance Staff, three WECC Consultants (Independent Contractors), and two NERC Staff members. FERC did not observe this audit.

The audit began the afternoon of December 10, with short presentations from SMUD and the WECC Compliance Staff. The audit then proceeded each day thereafter, and on December 14, the audit concluded in the afternoon with the preliminary audit findings presented to SMUD personnel in an exit briefing.

The audit scope involved the review of fifty-two (52) NERC Reliability Standards. No WECC Regional Reliability Standards were reviewed during this audit.

SMUD had self-reported twenty-nine (29) outstanding compliance violations and submitted Mitigation Plans for each one prior to the start of this audit. SMUD subsequently retracted one Mitigation Plan (EOP-001-0). The Audit Team reviewed SMUD's Mitigation Plans and Mitigation Plan Completion Forms for these outstanding compliance violations.

This audit report includes information for SMUD regarding the possible compliance violations. This information will be used to help determine the severity level of sanctions and penalties.

The Audit Team found possible violations with twenty (20) Requirements in twelve (12) of the fifty-two (52) total Reliability Standards reviewed during the audit. These possible violations along with this on-site Compliance Audit Report will be provided to the WECC Compliance Staff for processing by the WECC Compliance Monitoring and Enforcement Program (CMEP). If the WECC Compliance Department determines that any of the possible compliance violations are Alleged Violations, SMUD and NERC will be notified via an Alleged Violation Letter.

The Audit Team used the Reliability Standard Audit Worksheets (RSAW) during the documentation review of each Reliability Standard. (Note: Several Reliability Standards that were reviewed did not have a developed RSAW. For these standards the Requirements and Measurements of the standards were relied on for review metrics).

The Audit Team used the evidence (documentation provided and interviews) as the factual basis to support the audit findings and conclusions.

The WECC Audit Team reviewed SMUD's documentation and interviewed various SMUD personnel, focusing primarily on the 2006 to 2007 timeframe.

The Audit Team feels SMUD has a reliable and well run operation. The SMUD documentation was well organized. SMUD personnel made an outstanding effort to provide additional information as requested in interviews during the audit.

SMUD has made a good effort to identify deficiencies and implement mitigation plans.

SMUD is developing and implementing an Internal Compliance Program that is supported at all management levels:

- The plan is currently being developed, and
- Positions are budgeted but not filled.

The Audit Team found one major concern during the audit: Clearance 1 Distances are not identified in the Transmission Vegetation Management Program (TVMP for FAC-003-1).

This concern and the other information in this section are described in detail in the Findings Table below.

As background FERC Order 693, which was issued on March 16, 2007, made adherence to eighty-three (83) of the NERC Reliability Standards mandatory and enforceable in the United States on June 18, 2007. These 83 standards are subject to the sanctions guidelines effective on this date. It should be noted that this SMUD On-Site Compliance Audit was completed after the June 18, 2007 date. Therefore, compliance to the Reliability Standards is mandatory under the FERC Order.

<http://www.nerc.com/filez/enforcement/index.html>

AUDIT PROCESS

The compliance audit process steps are detailed in the NERC Compliance Monitoring and Enforcement Program (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.¹ The audit objectives are:

- Independently review SMUD's compliance with the requirements of the reliability standards that are applicable to SMUD based on the SMUD registered functions.
- Validate compliance with applicable reliability standards from the NERC 2007 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 standards, and review the status of associated mitigation plans.
- Document SMUD's compliance culture.
- Validate compliance with several standards in addition to the NERC 2007 Implementation Plan list of actively monitored standards (SMUD had submitted self-reported non-compliance and Mitigation Plans for a number of standards in addition to the NERC 2007 Implementation Plan list of actively monitored standards).
- Validate compliance to regional standards; however, no WECC Regional Reliability Standards were reviewed during this audit.

Scope

A compliance audit will include all reliability standards applicable to the registered entity monitored in the NERC Implementation Plans in the current and two previous years, and may include other reliability standards applicable to the registered entity. The scope of an on-site compliance audit can vary depending on whether it is scheduled as part of a regular, periodic scheduled audit or as part of a compliance investigation.

Note: For the 2007 compliance program, the monitoring period for the compliance audit will be the past 12 months or periods specified in individual reliability standards. The monitoring period is not limited to the time period for which penalties and sanctions are assessed.

The SMUD audit scope involved the review of fifty-two (52) NERC Reliability Standards. No WECC Regional Reliability Standards were reviewed during this audit.

Confidentiality and Conflict of Interest

Confidentiality agreements, executed by the three WECC Consultants (independent contractors) and code of conduct documentation for the two NERC representatives and WECC Compliance Staff, were provided to SMUD in advance of the audit. Work history

¹ North American Electric Reliability Corporation CMEP, paragraph 3.1, Compliance Audits

and conflict of interest forms submitted by each audit team member were also provided to SMUD. SMUD 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. SMUD accepted the audit team member participants with no objections.

On-site Audit

On-site audits of Reliability Coordinators (RCs), Balancing Authorities (BAs), and Transmission Operators (TOPs) are conducted on a three-year cycle. SMUD is registered as a BA, TOP, and many other functions, and is therefore subject to an on-site audit every three years.

In a pre-audit letter SMUD was officially notified of the December 10-14, 2007, on-site audit (60 day notice of audit). Accompanying this notification were several documents relating to the audit (pre-audit survey, audit scope, list of reliability standards, audit agenda overview, and request for evidence list):

SMUD was notified in the pre-audit letter that personnel (subject matter experts representing all the registered functions) would need to be available to answer questions (interviews) the audit team might have regarding the documentation.

Methodology

Methodology: the auditing standards and best practices that are to be followed by compliance auditors in carrying out their work as described in the Compliance Auditor Manual. The criteria should be objective, measurable, complete and relevant to the audit objectives. The auditor should identify potential sources of audit evidence and consider the amount and type of evidence needed given the risk and significance when defining the audit methodology.

Audit Overview

Depending on the size of the entity being audited, the on-site audits typically begin at 1:00 PM on a Monday and conclude with an exit briefing around 3:00 PM on Friday.

The audit overview meeting in the afternoon of the first day was the initial meeting between the audit team and SMUD personnel.

The meeting provided the audit team with a good overview of SMUD's operation and organization prior to actually beginning the audit process.

Audit

The audit began the afternoon of December 10, with short presentations from SMUD and the WECC Compliance Staff.

SMUD personnel provided an overview of SMUD's system and organization. SMUD generates, transmits, and distributes electricity to a 900 square-mile service area that includes Sacramento County and a small portion of Placer County in California.

The audit team leader provided an overview of the on-site audit process and how each standard would be validated using SMUD's submitted documentation. WECC also explained that interviews would be necessary if the audit team members required more information along with additional documentation on any standard. SMUD had submitted a number of self-reported violations and Mitigation Plans prior to the June 18, 2007, mandatory date and it was explained that the audit team would be evaluating these self-reported violations, Mitigation Plans and Mitigation Plan Completion Forms as necessary to complete the audit.

The audit then proceeded each day thereafter with adjustments to the agenda to accommodate interviews and to receive additional documentation. The audit team broke into three sub-teams of two auditors each in order to complete the auditing of the evidence. At least twice a day, the audit team recapped their preliminary findings to ensure the whole team concurred with each sub-team's findings.

SMUD was very flexible in having subject matter experts available for interviews and several subject matter experts were interviewed during the audit. The interviews were conducted in adjacent conference rooms and not in the main audit room.

The audit team's process for validating compliance used the evidence submitted by SMUD, the requested additional evidence, and interviews. After reviewing all the evidence from documentation and interviews, the audit team determined the existence of possible violations.

On December 14, the audit concluded in the afternoon with the preliminary audit findings presented to SMUD personnel in an exit briefing.

Exit Briefing

The exit briefing with SMUD personnel from all levels of the company was conducted during the afternoon of December 14. The closing presentation of preliminary findings was given by WECC, using Power Point slides. The presentation included a summary of the preliminary audit findings and audit team comments on the evidence provided. Each standard was then presented with the audit team's preliminary findings. At the end of the standards presentation, a summary of the audit process was explained, including the process of possible violations becoming alleged violations, SMUD's

options during the process, and the development and timing of the draft and final audit reports.

Company Profile

The Sacramento Municipal Utility District (SMUD) is the nation's sixth-largest community-owned electric utility.

The SMUD Balancing Area (BA) includes the 900 square-mile service area of Sacramento County and a small portion of Placer County in California, as well as up to the California-Oregon Border, and as far south as Modesto, California.

Audit Specifics

The compliance audit was conducted on December 10-14, 2007, at SMUD's main office in Sacramento, California.

Audit Team

Audit Team Role	Title	Company
Lead	Director of Compliance	WECC
Member	Senior Compliance Engineer	WECC
Member	Senior Compliance Engineer	WECC
Member	Regional Compliance Program Coordinator	NERC
Member	Manager of Compliance Administration	WECC
Observer	Compliance Data Analyst	WECC
Member	Consultant	WECC
Member	Consultant	WECC
Member	Consultant	WECC
Observer	Standards Development Coordinator	NERC

SMUD Audit Participants

Title	SMUD Organization
Supervisor, Power Operations Engineering	SMUD
Compliance Officer	SMUD
Principal Power Operations Engineer	SMUD
Principal Power Operations Engineer	SMUD
Principle Operations Engineer	SMUD
Supervisor of Operations Management Systems	SMUD
Shift Senior Power System Operator	SMUD
Supervisor, Power Systems Assessments	SMUD
Supervisor Distribution Planning	SMUD
Supervisor Vegetation Management Process	Vegetation Management, Distribution Services, SMUD
Power System Operations Scheduling/OASIS Support	SMUD
Power System Operator	SMUD
Senior Protection	SMUD

Title	SMUD Organization
Engineer	
Acting Supervisor for System Protection and Control	SMUD
Principal Transmission Planner	SMUD
Supervisor, Engineering Power Generation	SMUD
Superintendent, Thermal Generation & Gas Pipeline Assets Power Generation Department	SMUD

AUDIT RESULTS

The audit team reviewed and validated all the SMUD evidence, including additional evidence requested during the audit.

- The audit team took significant time to review the evidence that supported the significant judgments, findings, and conclusions. Extensive review of procedures, descriptions of processes, transactions and records was conducted.
- Decisions were made by the audit team during the overall assessment of evidence, and included assessment of whether the information was sufficient and appropriate.
- Communications with SMUD management was ongoing during the audit.
- The status of mitigation plans in progress, previous violations, and completed mitigation plans were all used in the validation of each standard as appropriate.
- SMUD had self-reported twenty nine outstanding compliance violations and submitted Mitigation Plans for each one prior to the start of this audit. One of the Mitigation Plans was retracted (EOP-001-0).
- Reliability Standard Audit Worksheets (RSAW), mitigation plans & completions, and summaries of auditor notes from interviews were used to validate compliance with each standard and to complete the Findings for the audit.

- This audit report includes information for SMUD regarding the possible compliance violations. This information will be used to help determine the severity level of sanctions and penalties.

Findings

Findings Table for SMUD Audit

The Finding column in the table below contains one or more of the following: Compliant, NA (Not Applicable), Not Audited, Possible Violation, Self-reported Violation (Self-Report), or other appropriate description.

Reliability Standard	Requirement	Finding
BAL-001-0	R1	Compliant
	R2	Compliant
	R3.	NA
	R4.	NA
BAL-002-0	R1.	Compliant
	R2.	NA
	R3.	Compliant
	R4.	Compliant
	R5.	NA
	R6.	Compliant
BAL-003-0	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	NA
	R5.	Compliant
	R6.	NA
BAL-006-1	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Compliant
CIP-001-1	R1.	Possible Violation (New): Self-Report
	R2.	Self-Report: Compliant
	R3.	Self-Report: Compliant

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

	R4.	Self-Report: Compliant
CIP-002-1 through CIP-009-1	.	Not Audited
COM-001-1	R1.	Compliant
	R2.	Self-Report: Compliant
	R3.	Self-Report: Compliant
	R4.	Compliant
	R5.	Compliant
	R6.	NA
COM-002-2	R1.	Compliant
	R2.	Compliant
EOP-001-0	R1.	Possible Violation: Self-Report Withdrawn
	R2.	NA
	R3.	Compliant
	R4.	Possible Violation
	R5.	Compliant
	R6.	Self-report: Compliant
	R7.	Possible Violation
EOP-002-2	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Compliant
	R6.	Compliant
	R7..	Compliant
	R8. .	NA
	R9..	NA
EOP-003-1	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4. .	Compliant
	R5.	Compliant

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

	R6.	Compliant
	R7.	Compliant
	R8.	Compliant
EOP-005-1	R1.	Compliant
	R2..	Self-Report: Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Compliant
	R6..	Compliant
	R7.	Compliant
	R8..	Compliant
	R9.	Compliant
	R10.	Compliant
	R11..	Compliant
EOP-008-0	R1.	Self-Report: Compliant
EOP-009-0	R1.	Compliant
	R2.	Self-Report: Compliant
FAC-001-0	R1.	Possible Violation
	R2.	Possible Violation
	R3.	Possible Violation
FAC-003-1	R1.	Possible Violation
	R2.	Compliant
	R3.	Compliant
	R4.	NA
FAC-008-1	R1.	Possible Violation: Self-Report
	R2.	Possible Violation: Self-Report
	R3.	Possible Violation: Self-Report
FAC-009-1	R1.	Possible Violation: Self-Report
	R2.	Compliant

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

FAC-010-1	R1.	Possible Violation: Self-report Incomplete
	R2.	Possible Violation
	R3.	Possible Violation
	R4.	Possible Violation
	R5.	Possible Violation
INT-006-2	R1.	Possible Violation: Self-Report
IRO-001-1	R1.	NA
	R2..	NA
	R3.	Compliant
	R4.	NA
	R5.	NA
	R6.	NA
	R7.	NA
	R8.	Compliant
	R9.	NA
IRO-004-1	R1.	NA
	R2.	NA
	R3.	NA
	R4.	Self-Report: Compliant
	R5.	NA
	R6.	NA
	R7.	Compliant
IRO-005-2	R1.	Self-report: NA
	R2.	NA
	R3..	NA
	R4.	NA
	R5.	NA
	R6.	NA
	R7.	NA
	R8.	Compliant
	R9..	NA
	R10.	NA

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

	R11.	NA
	R12.	Possible Violation
	R13.	Possible Violation
	R14.	Compliant
	R15.	NA
	R16.	NA
	R17.	NA
IRO-006-3	R1.	NA
	R2.	NA
	R3.	NA
	R4.	NA
	R5.	NA
	R6.	Compliant
MOD-006-0	R1.	Self-Report: Compliant
	R2.	Compliant
MOD-010-0	R1.	Compliant
	R2.	Compliant
MOD-012-0	R1.	Compliant
	R2.	Compliant
PER-001-0	R1.	Self-Report: Compliant
PER-002-0	R1.	Possible Violation: Self-Report
	R2.	Possible Violation: Self-Report
	R3.	Possible Violation: Self-Report
	R4.	Compliant
PER-003-0	R1.	Self-Report: Compliant
PRC-001-1	R1.	Self-report: Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Possible Violation
	R5.	Possible Violation: Self-Report
	R6.	Self-Report: Compliant

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

PRC-004-1	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
PRC-005-1	R1.	Possible Violation: Self-report
	R2.	Possible Violation: Self-Report
PRC-007-0	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
PRC-008-0	R1.	Self-Report: Compliant
	R2.	Compliant
PRC-010-0	R1.	Compliant
	R2.	Compliant
PRC-011-0	R1.	Self-Report: Compliant
	R2.	Compliant
PRC-016-0	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
PRC-017-0	R1.	Possible Violation
	R2.	Compliant
PRC-021-1	R1.	Compliant
	R2.	Compliant
TOP-001-1	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Compliant
	R6.	Possible Violation
	R7.	Compliant
	R8.	Compliant

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

TOP-002-2	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Compliant
	R6.	Compliant
	R7.	Compliant
	R8.	Compliant
	R9.	Compliant
	R10.	Self-Report: Compliant
	R11.	Compliant
	R12.	Compliant
	R13.	Compliant
	R14.	Compliant
	R15.	Compliant
	R16.	Self-Report: Compliant
	R17.	Self-Report: Compliant
	R18.	Compliant
	R19.	Compliant
TOP-003-0	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	NA
TOP-004-1	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
	R4.	Compliant
	R5.	Possible Violation
	R6.	Compliant
TOP-005-1	R1.	Self-Report: Compliant
	R2.	NA
	R3.	Self-Report: Compliant

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

	R4.	Compliant
TOP-006-1	R1.	Possible Violation: Self-Report
	R2.	Compliant
	R3.	Possible Violation: Self-Report
	R4.	Compliant
	R5.	Compliant
	R6.	Compliant
	R7.	Compliant
TOP-007-0	R1.	Self-Report: Compliant
	R2.	NA
	R3..	NA
	R4.	NA
TPL-001-0	R1.	Compliant
	R2.	Compliant
	R3.	Compliant
TPL-002-0	R1.	Possible Violation
	R2.	Compliant
	R3.	Compliant
TPL-003-0	R1.	Possible Violation
	R2.	Compliant
	R3.	Compliant
TPL-004-0	R1.	Compliant
	R2.	Compliant

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

VAR-001-1	R1.	Self-Report: Compliant
	R2.	Compliant
	R3.	Self-Report: Compliant
	R4.	Self-Report: Compliant
	R5.	Compliant
	R6.	Self-Report: Compliant
	R7.	Compliant
	R8.	Compliant
	R9.	Compliant
	R10.	Self-Report: Compliant
	R11.	Self-Report: Compliant
	R12.	Compliant
VAR-002-1	R1.	Self-Report: Compliant
	R2.	Self-Report: Compliant
	R3.	Self-Report: Compliant
	R4.	Compliant
	R5.	Compliant

COMPLIANCE CULTURE

SMUD's compliance culture was reviewed by the audit team.

SMUD is developing and implementing an Internal Compliance Program that is supported at all management levels:

The plan is currently being developed, and positions are budgeted but not filled.