



Western Electricity Coordinating Council

Compliance Audit Report Public

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

**Farmington Electric Utility System
(FEUS)
NCR05155**

Audit Dates: February 11-15, 2008

Final – June 3, 2010

TABLE OF CONTENTS

Executive Summary	3
Audit Process	4
Objectives	4
Scope	4
Confidentiality and Conflict of Interest	4
On-site Audit	5
Methodology	6
Audit Overview	6
Audit	7
Exit Briefing	7
Company Profile	7
Audit Specifics	7
Audit Results	8
Findings	9
Compliance Culture	14

Executive Summary

The WECC Compliance Department conducted an on-site compliance audit of the Farmington Electric Utility System (FEUS) on February 11-15, 2008. The audit was conducted at the FEUS headquarters in Farmington, New Mexico. The eight (8) member audit team was made up of four (4) WECC compliance staff, two (2) WECC consultants (independent contractors), and two (2) NERC staff members. FERC did not observe this audit.

The audit began at approximately 1:00 PM on February 11 with introductions and a short presentation by the WECC audit team about the audit process. FEUS leadership then presented an overview of the Company. The audit then proceeded each day thereafter, concluding in the early afternoon on Friday, February 15, with an exit briefing on the preliminary audit findings to FEUS personnel.

The audit scope involved the audit of forty-five (45) NERC Reliability Standards and two (2) WECC Regional Reliability Standards.

Prior to the start of the audit, FEUS self-reported thirty-seven (37) possible compliance violations, and submitted mitigation plans for each one. The audit team reviewed FEUS's mitigation plans and mitigation plan completion forms to determine compliance for these outstanding violations. The WECC Compliance Department will send formal documentation of the mitigation plans review status.

The audit team used the Reliability Standard Audit Worksheets (RSAW) during the compliance review of each reliability standard. Note: Some reliability standards do not have a developed RSAW. For these reliability standards the requirements for each standard were relied on for compliance review. The audit team used the evidence (documentation provided and interviews) as the factual basis to support audit findings and conclusions.

The audit team looked at compliance during the on-site audit for the 2006-2008 historical period of time and the audit does not reflect any corrective actions FEUS may have taken to mitigate historical violations.

As background, FERC Order 693 was issued on March 16, 2007, and made compliance to eighty-three (83) of the NERC Reliability Standards mandatory and enforceable in the United States on June 18, 2007. Each of these reliability standards is subject to the sanctions guidelines effective on this date. Note: the FEUS on-site compliance audit was completed after June 18, 2007.

http://www.nerc.com/filez/enforcement/FinalFiled_NOP_NOC-234.pdf

Audit Process

The compliance audit process steps are detailed in both the WECC and the NERC Compliance Monitoring and Enforcement Program (CMEP).

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 FEUS's compliance with the requirements of the reliability standards that are applicable to FEUS based on FEUS's registered functions.
- Validate compliance with applicable reliability standards from the NERC 2008 Implementation Plan list of actively monitored reliability standards.
- Validate compliance to WECC regional 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 FEUS's compliance culture and Internal Compliance Program.

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 2008 compliance program, the monitoring period for the compliance audit will be the past twenty-four (24) 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 FEUS audit scope involved the audit of forty-five (45) NERC Reliability Standards and two (2) WECC Regional Reliability Standards.

Confidentiality and Conflict of Interest

Confidentiality agreements executed by the NERC representatives and WECC staff were available to FEUS upon request. Work history and conflict of interest

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

forms submitted by each audit team member were provided to FEUS. FEUS 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. FEUS 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. FEUS is registered as a TOP, TO, GOP, GO, RP, PSE, LSE and DP; and is therefore, subject to an on-site audit every three (3) years.

FEUS was officially notified of the February 11-15, 2008, on-site audit (60-day notice of audit). Accompanying this notification were several documents relating to the audit as listed below:

- Pre-audit survey
- Audit scope
- List of reliability standards
- Audit agenda overview
- Request for evidence list
- Pre-Audit and Data Request Letter
- Registered Entity Introduction Letter (An explanation of Compliance Monitoring Authority and Registered Entity Obligations regarding collection of data and information necessary to assess compliance with approved reliability standards)
- 2008 WECC On-site Compliance Audit Team Bios
- NERC Reliability Standards
- Audit Questionnaire
- Audit Documentation Matrix.

FEUS 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.

The audit team had the flexibility to expand the scope of the audit by notifying FEUS in advance via the agenda that additions to the initial scope of the audit would be requested by the audit team leader if necessary during the audit overview meeting between the audit team and FEUS.

The Audit Documentation Matrix was completed by FEUS and sent to WECC approximately five (5) days ahead of the on-site audit. This matrix provided guidance to the audit team on where to look in the documentation for compliance to each of the reliability standards.

FEUS was also informed that the on-site compliance audit would be conducted consistent with the following WECC Regional and NERC documents:

- WECC Compliance Monitoring and Enforcement Program
- NERC Compliance Auditor Manual
- NERC Reliability Standard Audit Worksheets.

Professional judgment was used by the audit team during the on-site audit. The audit team leader requested interviews with FEUS employees representing subject matter expertise regarding all of the registered functions of FEUS. These interviews in conjunction with FEUS evidence, gave the audit team a factual basis for determining compliance with the NERC reliability standards.

Reference - Generally accepted government auditing standard 3.31 - Auditors must use professional judgment in planning and performing audits and attestation engagements and in reporting the results.

Reference - Generally accepted government auditing standard 3.39 - While this standard places responsibility on each auditor and audit organization to exercise professional judgment in planning and performing an audit or attestation engagement, it does not imply unlimited responsibility, nor does it imply infallibility on the part of either the individual auditor or the audit organization. Absolute assurance is not attainable because of the nature of evidence and the characteristics of fraud. Professional judgment does not mean eliminating all possible limitations or weaknesses associated with a specific audit, but rather identifying, considering, minimizing, mitigating, and explaining them.

Methodology

Methodology: the auditing reliability standards and best practices that are to be followed by compliance auditors in carrying out their work. The methodology should be objective, measurable, complete and relevant to the audit objectives. The auditors 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 meeting also provided the audit team with a good overview of FEUS's operation and organization prior to actually beginning the audit process.

Audit

The audit began at approximately 1:00 PM on February 11 with short presentations from the WECC Compliance Staff and FEUS.

The audit then proceeded each day thereafter with adjustments in the accommodations for the audit team, to the agenda to accommodate interviews, and to receive additional documentation. The audit team broke into sub-teams of two (2) auditors each in order to complete the auditing of each reliability standard. At least twice a day, the audit team recapped the preliminary findings to ensure the whole team concurred with each sub-team's findings.

FEUS 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.

On February 15, the audit concluded in the early afternoon with the preliminary audit findings presented to FEUS personnel in an exit briefing.

Exit Briefing

The exit briefing with FEUS personnel was conducted during the mid-afternoon on February 15. The closing presentation of preliminary findings was given by the audit team leader.

FEUS personnel did not have any comments during the exit briefing presentation.

Company Profile

The Farmington Electric Utility System is owned by the City of Farmington. FUES is an enterprise fund, hence not tax-funded in any way.

FEUS is located in the northwest corner of the state of New Mexico and is interconnected with PNM, Western, TSGT and the City of Aztec.

The FEUS system is comprised of 220 miles of 115 kV and 69 kV transmission serving approximately 43,000 customers.

Audit Specifics

The FUES compliance audit was conducted on February 11-15, 2008, at the FEUS headquarters in Farmington, New Mexico.

Audit Team

Audit Team Role	Title	Company
Lead	Senior Compliance Engineer	WECC
Member	Senior Compliance Engineer	WECC
Member	Senior Compliance Engineer	WECC
Member	Compliance Program Coordinator	WECC
Member	Regional Compliance Program Coordinator	NERC
Observer	Regional Compliance Program Coordinator	NERC
Member	Consultant	WECC
Member	Consultant	WECC

FEUS Audit Participants

Title	FEUS Organization
Electric Utility Director	FEUS
Superintendent of Technical Services	FEUS
(New) Compliance Engineer	FEUS
System Operations Supervisor	FEUS
System Protection Engineer	FEUS
Generation Manager	FEUS
Engineering Supervisor	FEUS
Compliance Engineer	FEUS
Senior System Operator	FEUS

Audit Results

The audit team reviewed and validated all the FEUS evidence, including additional evidence requested during the on-site audit and interviews with FEUS subject matter experts.

- The audit team spent significant time reviewing the evidence, findings, and conclusions. An extensive review of FEUS procedures, descriptions of processes, transactions and records was also conducted.
- Professional judgments were made by the audit team during the overall assessment of the evidence, and included a determination of whether the evidence was sufficient and appropriate to confirm compliance with the NERC Reliability Standards.
- The audit team found no major BES reliability concerns during the audit.
- Communications with FEUS management was ongoing during the audit.
- The status of mitigation plans in progress, self-reported violations, and completed mitigation plans were all evaluated during the audit.

- Prior to the audit, FEUS self-reported thirty-seven (37) outstanding compliance violations and submitted mitigation plans for each of them.
- Reliability Standard Audit Worksheets (RSAW), mitigation plans & completions, and summaries of auditor notes from interviews were used to validate compliance with each reliability standard and to complete the Findings for the audit.
- This audit report includes information regarding the possible compliance violations. This information will be used to help determine the severity level of sanctions and penalties.

Findings

The “Finding” column contains one of the following: Compliant, Possible Violation, Not Applicable (NA), Self-reported Violation (Self-Report), Outstanding Violation (OV), or other appropriate description.

Reliability Standard	Requirement	Finding
BAL-005-0	R1.	Compliant
BAL-005-0	R2.	NA
BAL-005-0	R3.	NA
BAL-005-0	R4.	NA
BAL-005-0	R5.	NA
BAL-005-0	R6.	NA
BAL-005-0	R7.	NA
BAL-005-0	R8.	NA
BAL-005-0	R9.	NA
BAL-005-0	R10.	NA
BAL-005-0	R11.	NA
BAL-005-0	R12.	NA
BAL-005-0	R13.	NA
BAL-005-0	R14.	NA
BAL-005-0	R15.	NA
BAL-005-0	R16.	NA
BAL-005-0	R17.	NA
CIP-001-1	R1.	Compliant
CIP-001-1	R2.	Compliant
CIP-001-1	R3.	Compliant
CIP-001-1	R4.	Compliant
COM-001-1	R1.	Compliant
COM-001-1	R2.	Compliant
COM-001-1	R3.	Possible Violation
COM-001-1	R4.	Compliant
COM-001-1	R5.	Possible Violation

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

Reliability Standard	Requirement	Finding
COM-001-1	R6.	NA
COM-002-2	R1.	Compliant
COM-002-2	R2.	Possible Violation
EOP-001-0	R1.	NA
EOP-001-0	R2.	Compliant
EOP-001-0	R3.	OV
EOP-001-0	R4.	Possible Violation
EOP-001-0	R5.	Compliant
EOP-001-0	R6.	Compliant
EOP-001-0	R7.	Compliant
EOP-002-2	R1.	NA
EOP-002-2	R2.	NA
EOP-002-2	R3.	NA
EOP-002-2	R4.	NA
EOP-002-2	R5.	NA
EOP-002-2	R6.	NA
EOP-002-2	R7.	NA
EOP-002-2	R8.	NA
EOP-002-2	R9.	NA
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.	NA
EOP-004-1	R2.	Compliant
EOP-004-1	R3.	Compliant
EOP-004-1	R4.	NA
EOP-004-1	R5.	NA
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.	Possible Violation

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

Reliability Standard	Requirement	Finding
EOP-005-1	R11.	Compliant
EOP-008-0	R1.	Possible Violation
EOP-009-0	R1.	Possible Violation
EOP-009-0	R2.	Compliant
FAC-001-0	R1.	Compliant
FAC-001-0	R2.	Compliant
FAC-001-0	R3.	Not Audited
FAC-002-0	R1.	Compliant
FAC-002-0	R2.	Compliant
FAC-003-1	R1.	NA
FAC-003-1	R2.	NA
FAC-003-1	R3.	NA
FAC-003-1	R4.	NA
FAC-008-1	R1.	Compliant
FAC-008-1	R2.	Compliant
FAC-008-1	R3.	Compliant
FAC-009-1	R1.	Compliant
FAC-009-1	R2.	Compliant
INT-001-2	R1.	Compliant
INT-001-2	R2.	NA
INT-004-1	R1.	Compliant
INT-004-1	R2.	Compliant
IRO-001-1	R1.	NA
IRO-001-1	R2.	NA
IRO-001-1	R3.	NA
IRO-001-1	R4.	NA
IRO-001-1	R5.	NA
IRO-001-1	R6.	NA
IRO-001-1	R7.	NA
IRO-001-1	R8.	Compliant
IRO-001-1	R9.	NA
IRO-004-1	R1.	NA
IRO-004-1	R2.	NA
IRO-004-1	R3.	NA
IRO-004-1	R4.	Compliant
IRO-004-1	R5.	NA
IRO-004-1	R6.	NA
IRO-004-1	R7.	Compliant
IRO-005-1	R1.	NA
IRO-005-1	R2.	NA
IRO-005-1	R3.	NA
IRO-005-1	R4.	NA

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

Reliability Standard	Requirement	Finding
IRO-005-1	R5.	NA
IRO-005-1	R6.	NA
IRO-005-1	R7.	NA
IRO-005-1	R8.	Compliant
IRO-005-1	R9.	NA
IRO-005-1	R10.	NA
IRO-005-1	R11.	NA
IRO-005-1	R12.	Compliant
IRO-005-1	R13.	NA
IRO-005-1	R14.	NA
IRO-005-1	R15.	NA
IRO-005-1	R16.	NA
IRO-005-1	R17.	Compliant
IRO-006-3	R1.	NA
IRO-006-3	R2.	NA
IRO-006-3	R3.	NA
IRO-006-3	R4.	NA
IRO-006-3	R5.	NA
IRO-006-3	R6.	NA
IRO-STD-006-1	WR1.	Compliant
MOD-010-0	R1.	Compliant
MOD-010-0	R2.	Compliant
MOD-012-0	R1.	Compliant
MOD-012-0	R2.	Compliant
MOD-017-0	R1.	Compliant
MOD-018-0	R1.	Possible Violation
MOD-018-0	R2.	Not Audited
PER-001-0	R1.	Compliant
PER-002-0	R1.	Possible Violation
PER-002-0	R2.	Compliant
PER-002-0	R3.	Compliant
PER-002-0	R4.	Possible Violation
PER-003-0	R1.	Compliant
PRC-004-1	R1.	Possible Violation
PRC-004-1	R2.	Possible Violation
PRC-004-1	R3.	Undetermined
PRC-005-1	R1.	Possible Violation
PRC-005-1	R2.	Possible Violation
PRC-STD-005-1	WR1.	Possible Violation
PRC-007-0	R1.	Compliant
PRC-007-0	R2.	Compliant

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

Reliability Standard	Requirement	Finding
PRC-007-0	R3.	Compliant
PRC-008-0	R1.	Compliant
PRC-008-0	R2.	Possible Violation
PRC-010-0	R1.	NA
PRC-010-0	R2.	NA
PRC-011-0	R1.	NA
PRC-011-0	R2.	NA
PRC-016-0	R1.	Compliant
PRC-016-0	R2.	Compliant
PRC-016-0	R3.	Compliant
PRC-017-0	R1.	Compliant
PRC-017-0	R2.	Compliant
PRC-021-1	R1.	NA
PRC-021-1	R2.	NA
TOP-002-2	R1.	Compliant
TOP-002-2	R2.	Compliant
TOP-002-2	R3.	Possible Violation
TOP-002-2	R4.	Possible Violation
TOP-002-2	R5.	Compliant
TOP-002-2	R6.	Compliant
TOP-002-2	R7.	NA
TOP-002-2	R8.	NA
TOP-002-2	R9.	NA
TOP-002-2	R10.	Compliant
TOP-002-2	R11.	Possible Violation
TOP-002-2	R12.	NA
TOP-002-2	R13.	Compliant
TOP-002-2	R14.	Possible Violation
TOP-002-2	R15.	Compliant
TOP-002-2	R16.	Compliant
TOP-002-2	R17.	Possible Violation
TOP-002-2	R18.	Compliant
TOP-002-2	R19.	Compliant
TOP-003-0	R1.	Compliant
TOP-003-0	R2.	Compliant
TOP-003-0	R3.	Compliant
TOP-003-0	R4.	NA
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

Reliability Standard	Requirement	Finding
TOP-004-1	R6.	Compliant
TOP-005-1	R1.	Compliant
TOP-005-1	R2.	NA
TOP-005-1	R3.	Compliant
TOP-005-1	R4.	Compliant
TOP-007-0	R1.	Compliant
TOP-007-0	R2.	Compliant
TOP-007-0	R3.	Compliant
TOP-007-0	R4.	NA
VAR-001-1	R1.	Compliant
VAR-001-1	R2.	Compliant
VAR-001-1	R3.	Compliant
VAR-001-1	R4.	Compliant
VAR-001-1	R5.	Compliant
VAR-001-1	R6.	Compliant
VAR-001-1	R7.	Compliant
VAR-001-1	R8.	Compliant
VAR-001-1	R9.	Compliant
VAR-001-1	R10.	Compliant
VAR-001-1	R11.	Compliant
VAR-001-1	R12.	Compliant
VAR-002-1	R1.	Compliant
VAR-002-1	R2.	Compliant
VAR-002-1	R3.	Compliant
VAR-002-1	R4.	Compliant
VAR-002-1	R5.	Compliant

Compliance Culture

The FEUS Internal Compliance Program (ICP) was reviewed during this audit: