



# **Compliance Audit Report Public Version**

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

**Owensboro Municipal Utilities  
NCR01290  
November 5-6, 2008**

**January 8, 2009**

## TABLE OF CONTENTS

Executive Summary .....	3
Audit Process .....	4
<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> .....	6
<i>Exit Briefing</i> .....	6
<i>Company Profile</i> .....	6
<i>Audit Specifics</i> .....	6
Audit Results .....	7
<i>Findings</i> .....	7
<i>Compliance Culture</i> .....	13

## EXECUTIVE SUMMARY

This final compliance audit report is the public version. Confidential information (including privileged and critical energy infrastructure information) has been redacted from this report. The full final compliance audit report was submitted to the audited entity and NERC.

Owensboro Municipal Utilities (OMU) was audited November 5-6, 2008 for compliance with the requirements contained in the currently mandatory and enforceable Reliability Standards in the 2008 NERC Compliance Monitoring and Enforcement Program (CMEP) that are applicable to OMU's registered functions. OMU is registered with SERC Reliability Corporation (SERC) as a Generation Operator (GOP), Generation Owner (GO), Distribution Provider (DP), and a Load-Serving Entity (LSE). Twenty-one standards were selected and identified to OMU as subject to review during this audit. The audit focused on documents and other evidence provided to SERC by the staff of OMU, 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. OMU staff was requested to provide an informational presentation on their progress with implementation of Cyber Security Standards CIP-002-1 through CIP-009

OMU 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 OMU as subject to this audit. OMU staff responded by providing evidence in the form of reports, procedures, studies, and other documents. OMU 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 OMU was judged to be compliant. Likewise, if any of the requirements or sub-requirements were not fully met, then OMU was judged to have a possible violation of the standard. A score of 100% is required for compliance.

The audit team verified that OMU does not own or operate Underfrequency Load Shedding, Under Voltage Load Shedding, generators listed in the SERC Regional Blackstart Plan, nor Special Protection Systems and therefore, 7 of the 21 previously mentioned standards were not applicable. These standards were: EOP-009, PRC-008, PRC-010, PRC-011, PRC-016, PRC-017, and PRC -021.

The audit team reviewed the current status of an open mitigation plan regarding NERC Reliability Standard PRC-005-1, R1 and found their status to be possibly non-compliant. The plan was approved as submitted on December 18, 2007 by SERC Compliance Enforcement.

OMU was found to be in compliance with all but two of the standards that were audited. The audit team identified a possible violation of FAC-009 Establish and Communicate Facility Ratings, Requirement 1, and PRC-005-1 Transmission & Generation Protection System Maintenance & Testing, Requirement 1. This audit report includes information about how far OMU missed the requirements for the possible compliance violations, and will be used to help determine the severity level of sanctions and penalties. The possible compliance violations will be processed through the SERC CMEP, and any further actions related to possible compliance violations will be through that process.

A copy of the Notice Of Penalty (NOP) can be found at the following link:  
[http://www.nerc.com/filez/enforcement/FinalFiled\\_NOP\\_NOC-381.pdf](http://www.nerc.com/filez/enforcement/FinalFiled_NOP_NOC-381.pdf)

## AUDIT PROCESS

The compliance audit process steps are detailed in the NERC CMEP. The NERC CMEP generally conforms to the United States Government Accounting 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 OMU's compliance with the requirements of the reliability standards that are applicable to OMU based on their registered functions.
- Validate compliance with applicable reliability standards from the NERC 2008 Implementation Plan's 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 the OMU compliance culture.

### **Scope**

The scope of the audit of OMU included all monitored standards that are in the NERC 2008 CMEP. Based on the confirmed registration of OMU, 21 reliability standards were the focus of the compliance audit. Of these 21 standards, 7 standards (EOP-009-0, PRC-008, PRC-010, PRC-011, PRC-016, PRC-017, and PRC -021) were determined to be "Not Applicable" and are detailed in the Audit Results section.

Note: For the 2008 compliance program, the monitoring period for the compliance audit will generally 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.

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

Code of conduct documentation for the regional entity staff were provided to OMU in advance of the audit. Work history and conflict of interest forms submitted by each audit team member were provided to OMU upon request. OMU 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. OMU accepted the audit team member participants with no objections.

### **On-site Audit**

OMU was contacted by letter on May 9, 2008 by SERC staff. The letter provided OMU with their initial notification of their upcoming audit in 2008, 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 OMU both verify their currently registered functions and complete and return an attached Pre-Audit Survey within 30 days.

---

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

On August 12, 2008, SERC staff forwarded an Audit Detail Letter to OMU, again confirming the scheduled audit dates and confirming OMU's registered functions within SERC. The Audit Detail Letter also provided OMU with notice of the Standards in Audit Scope, Proposed Audit Schedule, Audit Team Roster (with industry affiliations), and requested that OMU Subject Matter Experts (SMEs) responsible for and knowledgeable of compliance submittals be available for interview during the audit. In addition to the Audit Detail Letter, OMU was provided with a Non-Disclosure Agreement Signature Verification for audit team members, a Pre-Audit Questionnaire, a list of "Documents to be Provided or Have Available", and Reliability Standard Auditor Worksheets (RSAWs) 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 was identified, and conducted the audit of OMU. The standards were grouped and scheduled for review to make the most efficient use of OMU staff's time. The Audit Team Leader (ATL) initiated dialogue on each standard requirement and requested compliance evidence. This evidence, and OMU's staff response, was documented. OMU staff was requested to show valid evidence of meeting each applicable requirement and sub-requirement contained in the 21 standards that had been previously identified by SERC to OMU as subject to this audit. OMU staff responded by providing evidence in the form of reports, procedures, studies, and other documents. OMU staff would then cite specific portions of the evidence that demonstrated compliance.

This evidence and the citations were documented by the scribe on the RSAWs, 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 OMU staff members until it was determined that each requirement was met by the cited evidence or other evidence offered.

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

### ***Audit Overview***

The ATL conducted a pre-audit briefing November 3, 2008 at 2:30 p.m. for the staff of OMU to finalize logistics, and to review the audit team's process and expectations. The full audit team arrived at the OMU offices at 2:48 p.m., November 5, 2008. Each member of the audit team was introduced and professional affiliation identified. The staff of OMU was introduced, and general housekeeping matters explained. The ATL began the session with an opening presentation. He reviewed the NERC compliance plan for 2008 in general, and how it applied to OMU specifically. The ATL introduced and reviewed the standards to be covered in the audit, and addressed both the expectations of OMU staff and the quality of evidence to be presented. The ATL also covered the basic procedure for the audit, and the bounding rules of conduct. OMU staff made a brief presentation describing OMU's corporate structure, compliance program and an informational overview of progress made toward implementation of the Cyber Security Standard requirements of CIP-002-1 through CIP-009-1.

### **Audit**

The review of standards started at 7:50 a.m., November 6, 2008. The audit team initially reviewed the registration status of OMU with entity staff to verify applicability of each standard. Each standard's audit began with a recitation of each requirement. OMU 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 was communicated to OMU 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 RSAW.

The review of all applicable standards was completed at 1:26 p.m., November 6, 2008, at which time 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 RSAW.

### **Exit Briefing**

The ATL presented an exit briefing to the assembled audit team and entity staff at 2:05 p.m., November 6, 2008. This was followed by an informal response and questions from the OMU 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 OMU staff, along with requesting that they fill out formal feedback forms for submission to NERC and SERC.

The audit team left the OMU meeting room at 2:45 p.m., November 6, 2008.

### **Company Profile**

Owensboro Municipal Utilities (OMU) is the largest municipal electric and water system in Kentucky, with more than 26,000 electric, 24,000 water, and 3,200 telecommunications customers. OMU is overseen by the five-member Owensboro Utility Commission, which is appointed by the mayor of Owensboro and is approved by the city commission.

### **Audit Specifics**

The compliance audit was conducted November 5 and 6, 2008 at the OMU office in Owensboro, Kentucky.

### **Audit Team**

<b>Audit Team Role</b>	<b>Title</b>	<b>Company</b>
Lead	Compliance & Reliability Specialist	SERC
Member	Senior Compliance Auditor	SERC
Member	Senior Compliance Auditor	SERC
Member	Compliance Auditor	SERC

### **OMU Audit Participants Title and Organization**

<b>Title</b>	<b>OMU Organization</b>
Director of Engineering & Operations	OMU

<b>Title</b>	<b>OMU Organization</b>
Substation Supervisor	OMU
Electronics & Instrumentation Supervisor	OMU
System Analyst E & O	OMU
T & D Engineering Manager	OMU
Principal, Consultant	GDS Associates

## AUDIT RESULTS

The audit team found OMU to be in compliance with all of the NERC Reliability Standards in the audit scope, with the exception of possible violations of NERC Reliability Standard FAC-009-1, Requirement 1 and PRC-005-1, Requirement 1. See the Findings Table below.

### *Findings*

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
BAL-001-0	R1.	N/A
BAL-001-0	R2.	N/A
BAL-001-0	R3.	N/A
BAL-001-0	R4.	N/A
BAL-002-0	R1.	N/A
BAL-002-0	R2.	N/A
BAL-002-0	R3.	N/A
BAL-002-0	R4.	N/A
BAL-002-0	R5.	N/A
BAL-002-0	R6.	N/A
BAL-003-0	R1.	N/A
BAL-003-0	R2.	N/A
BAL-003-0	R3.	N/A
BAL-003-0	R4.	N/A
BAL-003-0	R5.	N/A
BAL-003-0	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
BAL-005-0	R1.	Compliant
BAL-005-0	R2.	N/A
BAL-005-0	R3.	N/A
BAL-005-0	R4.	N/A
BAL-005-0	R5.	N/A
BAL-005-0	R6.	N/A
BAL-005-0	R7.	N/A
BAL-005-0	R8.	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-005-0	R9.	N/A
BAL-005-0	R10.	N/A
BAL-005-0	R11.	N/A
BAL-005-0	R12.	N/A
BAL-005-0	R13.	N/A
BAL-005-0	R14.	N/A
BAL-005-0	R15.	N/A
BAL-005-0	R16.	N/A
BAL-005-0	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	All	N/A
COM-001-1	R1.	N/A
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.	N/A
EOP-001-0	R2.	N/A
EOP-001-0	R3.	N/A
EOP-001-0	R4.	N/A
EOP-001-0	R5.	N/A
EOP-001-0	R6.	N/A
EOP-001-0	R7.	N/A
EOP-002-2	R1.	N/A
EOP-002-2	R2.	N/A
EOP-002-2	R3.	N/A
EOP-002-2	R4.	N/A
EOP-002-2	R5.	N/A
EOP-002-2	R6.	N/A
EOP-002-2	R7.	N/A
EOP-002-2	R8.	N/A

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	R9.	N/A
EOP-003-1	R1.	N/A
EOP-003-1	R2.	N/A
EOP-003-1	R3.	N/A
EOP-003-1	R4.	N/A
EOP-003-1	R5.	N/A
EOP-003-1	R6.	N/A
EOP-003-1	R7.	N/A
EOP-003-1	R8.	N/A
EOP-004-1	R1.	N/A
EOP-004-1	R2.	Compliant
EOP-004-1	R3.	Compliant
EOP-004-1	R4.	N/A
EOP-004-1	R5.	N/A
EOP-005-1	R1.	N/A
EOP-005-1	R2.	N/A
EOP-005-1	R3.	N/A
EOP-005-1	R4.	N/A
EOP-005-1	R5.	N/A
EOP-005-1	R6.	N/A
EOP-005-1	R7.	N/A
EOP-005-1	R8.	N/A
EOP-005-1	R9.	N/A
EOP-005-1	R10.	N/A
EOP-005-1	R11.	N/A
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.	N/A
EOP-009-0	R1.	N/A
EOP-009-0	R2.	N/A
FAC-003-1	R1.	N/A
FAC-003-1	R2.	N/A
FAC-003-1	R3.	N/A
FAC-003-1	R4.	N/A
FAC-008-1	R1.	Compliant
FAC-008-1	R2.	Compliant
FAC-008-1	R3.	Compliant
FAC-009-1	R1.	Possible Violation

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

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
FAC-009-1	R2.	Compliant
FAC-013-1	R1.	N/A
FAC-013-1	R2.	N/A
INT-001-2	R1.	N/A
INT-001-2	R2.	N/A
INT-003-2	R1.	N/A
INT-004-1	R1.	N/A
INT-004-1	R2.	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-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.	N/A
IRO-004-1	R4.	Compliant
IRO-004-1	R5.	N/A
IRO-004-1	R6.	N/A
IRO-004-1	R7.	N/A
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.	N/A
IRO-005-1	R9.	N/A
IRO-005-1	R10.	N/A
IRO-005-1	R11.	N/A
IRO-005-1	R12.	N/A
IRO-005-1	R13.	Compliant
IRO-005-1	R14.	N/A
IRO-005-1	R15.	N/A
IRO-005-1	R16.	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	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.	N/A
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
PER-002-0	R1.	N/A
PER-002-0	R2.	N/A
PER-002-0	R3.	N/A
PER-002-0	R4.	N/A
PER-003-0	R1.	N/A
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-004-1	R1.	Compliant
PRC-004-1	R2.	Compliant
PRC-004-1	R3.	Compliant
PRC-005-1	R1.	Possible Violation
PRC-005-1	R2.	Compliant
PRC-008-0	R1.	N/A
PRC-008-0	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-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

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

<b>Reliability Standard</b>	<b>Requirement</b>	<b>Finding</b>
PRC-021-1	R1.	N/A
PRC-021-1	R2.	N/A
TOP-002-2	R1.	N/A
TOP-002-2	R2.	N/A
TOP-002-2	R3.	Compliant
TOP-002-2	R4.	N/A
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.	N/A
TOP-002-2	R10.	N/A
TOP-002-2	R11.	N/A
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.	N/A
TOP-002-2	R17.	N/A
TOP-002-2	R18.	Compliant
TOP-002-2	R19.	N/A
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.	N/A
TOP-004-1	R2.	N/A
TOP-004-1	R3.	N/A
TOP-004-1	R4.	N/A
TOP-004-1	R5.	N/A
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-007-0	R1.	N/A
TOP-007-0	R2.	N/A
TOP-007-0	R3.	N/A
TOP-007-0	R4.	N/A
TPL-001-0	R1.	N/A
TPL-001-0	R2.	N/A
TPL-001-0	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>
TPL-002-0	R1.	N/A
TPL-002-0	R2.	N/A
TPL-002-0	R3.	N/A
TPL-003-0	R1.	N/A
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.	N/A
VAR-001-1	R2.	N/A
VAR-001-1	R3.	N/A
VAR-001-1	R4.	N/A
VAR-001-1	R5.	N/A
VAR-001-1	R6.	N/A
VAR-001-1	R7.	N/A
VAR-001-1	R8.	N/A
VAR-001-1	R9.	N/A
VAR-001-1	R10.	N/A
VAR-001-1	R11.	N/A
VAR-001-1	R12.	N/A
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**

Information regarding the compliance culture of OMU was obtained from the Pre-Audit Compliance Survey, Compliance Program Survey, and Pre-Audit Questionnaires that were completed by OMU prior to the audit.