Compliance Audit Report
Public Version

Henderson Municipal Power & Light
NCR01254
November 12-13, 2008

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

December 19, 2008

TABLE OF CONTENTS

Executive Summary 3

Audit Process 4

Objectives *4*

Scope *5*

Confidentiality and Conflict of Interest *5*

On-site Audit *5*

Methodology *5*

Audit Overview *6*

Audit *6*

Exit Briefing *6*

Company Profile *7*

Audit Specifics *7*

Audit Results 7

Findings *8*

Compliance Culture *14*

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.

Henderson Municipal Power and Light (HMPL) was audited November 12-13, 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 HMPL's registered functions. HMPL is registered with SERC Reliability Corporation (SERC) as a Transmission Owner (TO), Generation Owner (GO), Distribution Provider (DP) and a Load Serving Entity (LSE). Twenty standards were selected and identified to HMPL as subject to review during this audit. The audit focused on documents and other evidence provided to SERC by the staff of HMPL, 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. HMPL staff was requested to provide an informational presentation on their progress with implementation of Cyber Security Standards CIP-002-1 through CIP-009.

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

The audit team verified that HMPL does not own or operate Overhead Transmission Lines above 200 kV, Underfrequency Load Shedding, Under Voltage Load Shedding equipment, nor any generators listed in the SERC Regional Blackstart Plan, and therefore seven of the twenty previously mentioned standards were not applicable. These standards were: FAC-003, PRC-008, PRC-010, PRC-011, PRC-016, PRC-017 and PRC-021.

HMPL earlier self-reported a violation of PRC-005-1; Requirement 1 as a Generator Owner, and Requirement 2 as both a Generator Owner and a Transmission Owner. However, the audit team identified an additional Possible Violation since the documentation provided for the transmission system protective systems did not address intervals, basis, and M&T summaries for Associated Communications Systems, and DC Control Circuitry and CT's and PT's from June 18, 2007 to September 12, 2008. There was no basis for CT and PT Testing from June 18, 2007 to November 12, 2008. [Basis for change: HMPL PGP PRC005 Version 0 dated September 2, 2008 has M&T summaries and basis for intervals (based on electro-mechanical and microprocessor based testing.)] In addition there was no basis for the intervals for batteries and relays from June 18, 2007 to November 3, 2008. A procedure is currently being finalized to mitigate the earlier self-report and contains the necessary intervals, basis, and summaries for both the generation and transmission protective systems.

HMPL has self-reported possible violations of two standards, IRO-004-1 Requirement 4 and TOP-002-2 Requirement 3. The audit team reviewed these two standards and did not find evidence of possible violation above and beyond HMPL's initial self-reports. These two standards are shown as compliant in the Findings section, and are already in process by SERC Enforcement. HMPL was found by the audit team in Possible Violation of CIP-001-1, Requirement 1 the evidence presented was deficient in the following items: A gap in the compliance of HMPL between June 18, 2007 and July 23, 2008. The compliance gap was identified since no specific language was in an effective procedure for the communication of sabotage events to operating personnel or language addressing multi site sabotage. Procedure was revised and the possible violation addressed appropriately in a revision dated 07/23/08. HMPL was found by the audit team in Possible Violation of FAC-008-0, Requirement 1 because the evidence presented was deficient in the following items: A gap in compliance existed for HMPL from 6/18/07 to 9/12/08. Ratings for all facilities had been determined using documented acceptable methodologies, but these were not fully compliant with the requirement as written. Procedure was revised and the possible violation addressed appropriately in a revision dated 09/12/08.

HMPL was found to be in compliance with all but three of the standards that were audited. The audit team identified possible violations, in addition to those self-reported, of FAC-008-0 Facilities Rating Methodology, PRC-005-1 Transmission & Generation Protection System Maintenance & Testing, and CIP-001-1 Sabotage Reporting. This audit report includes information about how far HMPL 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-210.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.[1] The audit objectives are:

- Independently review HMPL's compliance with the requirements of the reliability standards that are applicable to HMPL 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 HMPL compliance culture.

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

Scope

The scope of the audit of HMPL included all monitored standards that are in the NERC 2008 CMEP. Based on the confirmed registration of HMPL, twenty Reliability Standards were the focus of the compliance audit. Of these twenty standards, seven standards (FAC-003, 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 HMPL in advance of the audit. Work history and conflict of interest forms submitted by each audit team member were provided to HMPL upon request. HMPL 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. HMPL accepted the audit team member participants with no objections.

On-site Audit

HMPL was contacted by letter on May 12, 2008 by SERC staff. The letter provided HMPL 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 HMPL both verify their currently registered functions and complete and return an attached Pre-Audit Survey within 30 days.

On August 15 2008, SERC staff forwarded an Audit Detail Letter to HMPL, again confirming the scheduled audit dates and confirming HMPL's registered functions within SERC. The Audit Detail Letter also provided HMPL with notice of the Standards in Audit Scope, Proposed Audit Schedule, Audit Team Roster (with industry affiliations), and requested that HMPL 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, HMPL 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 HMPL. The standards were grouped and scheduled for review to make the most efficient use of HMPL staff's time. The Audit Team Leader (ATL) initiated dialogue on each standard requirement and requested compliance evidence. This evidence, and HMPL's staff response, was documented. HMPL staff was requested to show valid evidence of meeting each applicable requirement and sub-requirement contained in the twenty standards that had been previously identified by SERC to HMPL as subject to this audit. HMPL staff responded by providing evidence in the form of reports, procedures, studies, and other documents. HMPL 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 HMPL 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 HMPL did not provide sufficient evidence to support a finding of compliance, then a possible violation was identified by the team and HMPL staff was informed.

Audit Overview

The full audit team arrived at the HMPL offices November 12, 2008 at 12:50pm. Each member of the audit team was introduced and professional affiliation identified. The staff of HMPL 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 HMPL specifically. The ATL introduced and reviewed the standards to be covered in the audit, and addressed both the expectations of HMPL 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. HMPL staff made a brief presentation describing HMPL'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 1:56pm November 12, 2008. The audit team initially reviewed the registration status of HMPL with entity staff to verify applicability of each standard. Each standard's audit began with a recitation of each requirement. HMPL 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 HMPL 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 10:29am November 13, 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 11:06am November 13, 2008. This was followed by an informal response and questions from the HMPL staff. The exit briefing summarized the team 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 HMPL staff, along with requesting that they fill out formal feedback forms for submission to NERC and SERC.

The audit team left the HMPL meeting room at 11:45pm November 13, 2008.

Company Profile

Henderson Municipal Power and Light (HMPL) is a municipal electric utility established under KRS chapter 96. HMP&L is governed by a five member citizen Utility Commission appointed by the City Commission. HMP&L owns Generation Station One and Generation Station Two which provide electric service to the Citizens of Henderson. The standard primary distribution voltage of the HMP&L system is 13.8 kV and HMP&L also has a very small area served by 2.4 kV. HMP&L provides service to a total of 12,593 meters in the City of Henderson. HMP&L has 10,317 residential customers as well as 2,276 commercial/demand customers. The HMP&L system has 69 and 161kV transmission facilities and ties with Big Rivers Electric Corporation at these voltage levels.

Audit Specifics

The compliance audit was conducted November 12 and 13, 2008 at the HMPL office in Henderson, Kentucky.

Audit Team

Audit Team Role	Title	Company
Lead	Compliance & Reliability Specialist	SERC
Member	Senior Compliance Auditor	SERC
Member	Senior Compliance Auditor	SERC
Member	Compliance Auditor	SERC

HMPL Audit Participants Title and Organization

Title	HMPL Organization
Power Production Director	HMPL
Line Supervisor	HMPL
Assistant to General Manager	HMPL
T & D Manager	HMPL
Communication Director	HMPL
HR Director	HMPL
Comptroller	HMPL
Project Manager, Transmission Services	GDS Associates

AUDIT RESULTS

The audit team found HMPL 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 and Requirement FAC-008-0 Requirement 1, PRC-005-1 Requirement 1, and CIP-001-1 Requirement 1. These possible violations were identified in addition to those already self-reported by HMPL prior to the audit. Please see the Findings Table below.

Findings

Reliability Standard	Requirement	Finding
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
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

Reliability Standard	Requirement	Finding
BAL-006-1	R4.	N/A
BAL-006-1	R5.	N/A
CIP-001-1	R1.	Possible Violation
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.	N/A
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
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

Reliability Standard	Requirement	Finding
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.	Possible Violation
FAC-008-1	R2.	Compliant
FAC-008-1	R3.	Compliant
FAC-009-1	R1.	Compliant
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

Reliability Standard	Requirement	Finding
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
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

Reliability Standard	Requirement	Finding
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
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.	N/A

Reliability Standard	Requirement	Finding
TOP-002-2	R14.	N/A
TOP-002-2	R15.	N/A
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.	N/A
TOP-003-0	R2.	N/A
TOP-003-0	R3.	N/A
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
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

Reliability Standard	Requirement	Finding
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.	N/A
VAR-002-1	R2.	N/A
VAR-002-1	R3.	N/A
VAR-002-1	R4.	Compliant
VAR-002-1	R5.	Compliant

Compliance Culture

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