NORTHEAST POWER COORDINATING COUNCIL, INC.
1040 AVE OF THE AMERICAS, NEW YORK, NY 10018 TELEPHONE (212) 840-1070 FAX (212) 302-2782

Compliance Audit Report
Public Version

New York Independent System Operator
NCR07160

August 18 to August 21, 2009

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

September 4, 2009

TABLE OF CONTENTS

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.

The on-site CIP compliance audit of New York Independent System Operator Inc. (NYISO), NERC ID #NCR07160 was conducted between August 18 and August 21, 2009. The audit was completed using data submitted by NYISO prior to the start of the on-site audit and data provided when the audit team arrived on-site and as a result of questions and data requests that arose during the audit.

The auditor evaluated NYISO's compliance with the 6 reliability standards and 13 requirements in the 2009 NERC Compliance Monitoring and Enforcement Program (CMEP). The audit reviewed reliability standards identified in the NERC 2009 Implementation Plan for the period of the last twelve months or monitoring timeframes specified in each reliability standard. In addition to the standards identified in the pre-audit letter, CIP-006-1 was also audited, due to its strong relationship to the other CIP standards and due to the availability of physical security expertise on the audit team. Although CIP-006-1 was not on the monitored list and NYISO was not made aware of the intention to audit the standard, they were judged compliant with all 6 of the requirements. Therefore, of the total of 7 standards and 19 requirements audited for the functions NYISO is registered, all standards and requirements were judged to be compliant.

CIP standards 2, 3, 4, 6, 7, 8 and 9 were audited. Evidence used to determine compliance with the CIP standards was judged to be sensitive; as a result, no evidence was removed from the NYISO site. A custody letter was put in place and copies of all evidence were placed in a sealed envelope in the possession of the Cyber Security Manager. The custody agreement allows NPCC access to the data at NYISO offices, if required, prior to conducting the next regularly scheduled audit in 2012. .

Oversight of the audit was provided by 3 FERC and 2 NERC staff members.

NYISO staff provided an overview of the IT infrastructure and its role in supporting operations prior to the beginning of the audit; in addition, a tour of the computer rooms revealed CCA equipment was marked with labels to raise staff awareness. As each standard was reviewed, the SME responsible provided overview specific to the particular standard, resulting in a more clear understanding of their business model and accelerating the audit process. The evidence provided to demonstrate compliance was well presented and well organized. The audit team would like to thank the NYISO staff for their support offered throughout the audit.

There were no ongoing or recently completed mitigation plans and, therefore, none were reviewed by the audit team.

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.[1] The audit objectives are to:

- Independently review New York Independent System Operator's compliance with the requirements of the CIP reliability standards that are applicable to NYISO based on NYISO's registered functions.
- Validate compliance with applicable CIP reliability standards from the NERC 2009 Implementation Plan list of actively monitored standards and additional NERC reliability standards selected by NERC.
- Validate compliance with applicable Regional Standards from the NPCC 2009 Implementation Plan list of actively monitored standards.
- Validate evidence of self-reported violations and previous self-certifications and confirm compliance with other requirements of the reliability standard.
- Review the status of associated mitigation plans.
- Observe and document New York Independent System Operator's compliance program and culture.

Scope

The audit included all standards identified in the May 12, 2009 audit letter. The audit was a regularly scheduled CIP audit and no self-reported violations or compliance investigations were involved in the audit.

Confidentiality and Conflict of Interest

Confidentiality and Conflict of Interest of the audit team are governed under the Delegation Agreement with NERC and Section 1500 of the NERC Rules of Procedure.
The audited entity was informed in advance of the audit that the independent contractors executed confidentiality agreements and code of conduct documentation was in place for the NERC representative and regional entity staff. Work history and conflict of interest forms submitted by each audit team member are on file in the NPCC corporate offices. The audited entity 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

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

member's impartial performance of duties. The audited entity accepted the audit team members with no objections.

On-site Audit

NYISO was provided with a pre-audit request letter identifying the standards and requirements subject to audit. The audit letter was sent to NYISO more than 60 days in advance of the scheduled audit. This was an on-site audit conducted every three years or as determined to be necessary by the region. NYISO had not self-reported any violations.

NYISO staff provided an overview of the IT infrastructure and its role in supporting operations, prior to the beginning of the audit. As each standard was reviewed, the SME responsible provided overview specific to the particular standard, resulting in a more clear understanding of their business model and accelerating the audit process. These interviews resulted in data requests that, in conjunction with the submitted evidence, provided the auditors with a basis for professional judgment when validating compliance with reliability standards.

Methodology

The auditors prepared reliability standards audit worksheets (RSAWs) to evaluate each standard. The RSAWs are used to ensure consistency and to document evidence of compliance or non-compliance with the standards. All relevant documents are considered and to the extent they form a portion of the audit trail are referenced in the RSAWs.

Audit Overview

The audit overview was provided to NYISO in both a conference call on August 4, 2009 between NPCC staff, FERC representatives, NERC representatives and NYISO representatives and on August 18, 2009 at the beginning of the audit. During the on-site kickoff meeting, each audit team member reviewed his or her career and noted they had signed confidentiality agreements. The FERC and NERC observers were introduced and provided brief comments on their roles in the audit. A brief explanation of the audit process was given and the timelines were discussed. NYISO was given an opportunity to reject the auditors but accepted the auditors and their credentials for this audit. NYISO introduced their team and made a presentation that provided an overview of the IT function.

Audit

Each member, prior to arriving at the site, reviewed all data submitted and produced a list of questions that required subject matter experts' responses. That team then did the on-site questioning and produced the RSAWs for the standard. All team members participated in the question process. Some questions were resolved using the data provided in advance of the audit and additional data provided on-site, and others were answered by follow-up data submittals during the site visit. Due to the sensitive nature of the data, the bulk of the data was provided when the team arrived on-site. Evidence used to determine compliance with the CIP standards was judged to be sensitive; as a result, no evidence was removed from the NYISO site. A

custody letter was put in place and copies of all evidence were placed in a sealed envelope in the possession of the Cyber Security Manager. The custody agreement allows NPCC access to the data at NYISO offices, if required, at a future date.

Exit Briefing

The exit briefing was conducted at the NYISO offices on August 21, 2009. The entire team of NPCC auditors, FERC and NERC observers, and NPCC staff attended. An audit presentation summarized the results of the audit**.** Of the 7 standards and 19 requirements audited for the functions NYISO is registered, all standards and requirements were judged to be compliant. NYISO commented that work associated with preparing for the audit and the audit helped them improve their own processes.

Company Profile

The New York Independent System Operator (NYISO) manages New York's electric transmission grid and administers the wholesale electricity markets for New York State. The NYISO is dedicated to being recognized as a leader in maintaining bulk power reliability through state-of-the-art processes and technology.

The NYISO recognizes the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability and the risks to which they are exposed. Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data.

Within the New York Control Area (NYCA) footprint, the NYISO provides reliability coordinator services to Bulk Power System asset owners. The NYISO does not own transmission or generating facilities. The NYISO is a not-for-profit, federally regulated entity charged with maintaining the reliability of the NYCA and administering the New York electricity markets. The NYISO performs its balancing authority functions from its control center located in Schenectady, NY. The NYISO also performs its transmission operator functions from that location. These services are for one balancing area, the NYCA, which is contiguous to the geographic boundaries of New York State.

Audit Specifics

The compliance audit was conducted from August 18 to August 21, 2009 at the NYISO offices in Albany, New York.

NPCC Audit Team Role	Title	Company
Regional staff	Manager Compliance	NPCC-Compliance Audit Program
Lead CIP Auditor	Engineer	NPCC-Compliance Audit Program

NPCC Audit Team Role	Title	Company
CIP Auditor	Compliance Specialist	NPCC-Compliance Audit Program
CIP Auditor	Contracted Consultant	NPCC-Compliance Audit Program
Compliance Auditor	Contracted Consultant	NPCC-Compliance Audit Program

FERC

Title	Division	Company
Chief, Audits Branch 2	Office of Enforcement	FERC
Auditor	Office of Enforcement	FERC
Energy Infrastructure and Cyber Security Advisor	Office of Electric Reliability	FERC

NERC

Title	Company
Regional Compliance Auditor	NERC
Regional Compliance Auditor	NERC

NYISO

Title	Organization
Supervisor, Reliability Compliance and Assessment	NYISO
Manager, Infrastructure Services	NYISO
Manager, Reliability Compliance and Industry Affairs	NYISO
Manager, Grid Operations	NYISO
Chief System Operator	NYISO
Supervisor, Enterprise Security	NYISO
Supervisor, Network Operations	NYISO
Supervising Senior Auditor	NYISO
Manager, Quality Control and Configuration Management	NYISO
President and CEO	NYISO
Vice President, CIO	NYISO
Vice President, Operations	NYISO
Vice President, Risk Management and Compliance	NYISO
Director, Internal Audit	NYISO

Audit Results

The on-site CIP compliance audit of New York Independent System Operator (NYISO) was conducted between August 18 and August 21, 2009. The audit was completed using data submitted by NYISO prior to the start of the on-site audit and data provided when the audit team arrived on-site and as a result of questions and data requests that arose during the audit.

The auditor evaluated NYISO's compliance with the 6 reliability standards and 13 requirements in the 2009 NERC Compliance Monitoring and Enforcement Program (CMEP). The audit reviewed reliability standards identified in the NERC 2009 Implementation Plan for the period of the last twelve months or monitoring timeframes specified in each reliability standard. In addition to the standards identified in the pre-audit letter, CIP-006-1 was also audited, due to its strong relationship to the other CIP standards and due to the availability of physical security expertise on the audit team. Although CIP-006-1 was not on the monitored list and NYISO was not made aware of the intention to audit the standard, they were judged compliant with all 6 of the requirements. Therefore, of the total of 7 standards and 19 requirements audited for the functions NYISO is registered, all standards and requirements were judged to be compliant.

CIP standards 2, 3, 4, 6, 7, 8 and 9 were audited. Evidence used to determine compliance with the CIP standards was judged to be sensitive; as a result, no evidence was removed from the NYISO site. A custody letter was put in place and copies of all evidence were placed in a sealed envelope in the possession of the Cyber Security Manager. The custody agreement allows NPCC access to the data at NYISO offices, if required, at a future date.

Oversight of the audit was provided by 3 FERC and 2 NERC staff members.

Findings

The following table details findings for compliance with the reliability standards listed in the NERC 2009 Implementation Plan.

Reliability Standard	Requirement	Finding
CIP-002-1	R1	Compliant
CIP-002-1	R2	Compliant
CIP-002-1	R3	Compliant
CIP-003-1	R1	Compliant
CIP-003-1	R2	Compliant
CIP-003-1	R3	Compliant
CIP-004-1	R2	Compliant
CIP-004-1	R3	Compliant
CIP-004-1	R4	Compliant
CIP-006-1	R1	Compliant
CIP-006-1	R2	Compliant
CIP-006-1	R3	Compliant

Reliability Standard	Requirement	Finding
CIP-006-1	R4	Compliant
CIP-006-1	R5	Compliant
CIP-006-1	R6	Compliant
CIP-007-1	R1	Compliant
CIP-008-1	R1	Compliant
CIP-009-1	R1	Compliant
CIP-009-1	R2	Compliant

Compliance Culture

The audit team reviewed New York Independent System Operators' compliance culture. During all contacts, NYISO staff was professional in their approach to compliance and understood the importance of the compliance and its role in maintaining reliability. NYISO's entire chain of command, from the CEO down, participated in the audit. It was clear that the NYISO was committed at all levels to the strong compliance program and the improved reliability resulting from such a program.