FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

In Reply Refer To:
Office of Enforcement
Docket No. PA11-21-000
November 1, 2012

Terry Boston, President and CEO
PJM Interconnection, L.L.C.
Valley Forge Corporate Center
955 Jefferson Ave.
Norristown, PA 19403

Dear Mr. Boston:

1. The Division of Audits within the Office of Enforcement, with the assistance of staff from the Office of Electric Reliability, has completed an audit of PJM Interconnection, L.L.C. (PJM) for the period from June 18, 2007 to July 18, 2012. The audit evaluated PJM's performance as: (1) a Table 1 entity responsible for certain Critical Infrastructure Protection Reliability Standards; and (2) a Transmission Operator and Transmission Planner. Personnel from the North American Electric Reliability Corporation, Reliability*First* Corporation, and SERC Reliability Corporation also participated as observers on the audit. The enclosed audit report explains our performance enhancement findings and recommendations.

2. In its September 27, 2012 response, PJM does not contest the performance enhancement findings and agrees with the associated recommendations. A copy of PJM's verbatim responses is included as an appendix to this report. I hereby approve the audit findings and recommendations. Within 30 days of this letter order, PJM should submit a plan to comply with the corrective actions. PJM should make quarterly filings describing how and when it plans to comply with the corrective actions, including the completion dates for each corrective action. The filings should be made no later than 30 days after the end of each calendar quarter, beginning with the first quarter after this audit report is issued, and continuing until all the corrective actions are completed.

3. The Commission delegated the authority to act on this matter to the Director of OE under 18 C.F.R. § 375.311 (2012). This letter order constitutes final agency action. PJM may file a request for rehearing with the Commission within 30 days of the date of this order under 18 C.F.R. § 385.713 (2012).

4. This letter order is without prejudice to the Commission's right to require hereafter any adjustments it may consider proper from additional information that may come to its attention. In addition, any instance of noncompliance not addressed herein or that may occur in the future may also be subject to investigation and appropriate remedies.

5. I greatly appreciate the courtesies extended to our staff. If you have any questions, please contact Mr. Bryan K. Craig, Director and Chief Accountant, Division of Audits at (202) 502-8741.

Sincerely,

Norman C. Bay
Director
Office of Enforcement

Enclosure

Federal Energy Regulatory Commission

Audit of the Performance of PJM Interconnection, L.L.C. as a Table 1 Entity Responsible for Certain CIP Reliability Standards, and as a NERC-Registered Transmission Operator and Transmission Planner.

Docket No. PA11-21-000
November 1, 2012

Office of Enforcement
Division of Audits

TABLE OF CONTENTS

I. Executive Summary

A. Overview

The Division of Audits within the Office of Enforcement, with the assistance of staff from the Office of Electric Reliability (OER) (collectively audit staff), has completed an audit of PJM Interconnection, L.L.C. (PJM). The audit was commenced to evaluate PJM's performance as: (1) a Table 1 entity responsible for certain Critical Infrastructure Protection (CIP) Reliability Standards; and (2) a Transmission Operator and Transmission Planner. Personnel from the North American Electric Reliability Corporation (NERC), Reliability*First* Corporation (Reliability*First*), and SERC Reliability Corporation (SERC) also participated as observers on the audit. The audit covered the period from June 18, 2007 to July 18, 2012.

B. PJM Interconnection, L.L.C.

PJM operates as a regional transmission organization responsible for the operation of wholesale electric markets, as well as for centrally dispatching electric systems in the PJM region. PJM coordinates a pooled generating capacity of approximately 185,600 megawatts and operates wholesale electricity markets with approximately 800 companies, which are eligible to transact in the markets administered by PJM. It enables the delivery of electric power to approximately 60 million people throughout all or parts of 13 states, as well as the District of Columbia.

PJM is registered in the Reliability*First* and SERC regions for the following reliability functions, as defined in the NERC Reliability Functional Model: Balancing Authority, Interchange Authority, Planning Coordinator, Reliability Coordinator, Resource Planner, Transmission Operator, Transmission Planner, and Transmission Service Provider. [1]

[1] The NERC Reliability Functional Model defines the set of functions that must be performed to ensure the reliability of the Bulk-Electric System (BES) and also explains the relationship between and among the entities responsible for performing the tasks within each function. The model provides the foundation and framework upon which NERC develops and maintains its Reliability Standards. NERC's Reliability Standards establish the requirements of the responsible entities that perform the functions defined in this model.

C. Summary of Findings and Recommendations

Audit staff's findings and recommendations are summarized below. A detailed discussion is included in section IV of this report.

1. Performance Enhancements

We found eight areas in which PJM could improve its performance:

- *Identifying Critical Cyber Assets Associated with Critical Assets* – PJM's process for identifying Critical Cyber Assets (CCAs) associated with its Critical Assets (CAs) needs to be enhanced to ensure that all CCAs related to the reliability or operability of the BES are properly identified.[2] These enhancements will help PJM ensure no potential gaps exist in its process for identifying the CCAs.

- *Access to Critical Cyber Assets* – PJM needs to improve its processes and procedures for managing employees' logical (i.e., electronic) access rights to CCAs for access changes and for terminating access rights of employees to CCAs.[3] PJM should improve its performance by eliminating its reliance on a decentralized, manual process for implementing change requests and removing employees' access rights to CCAs.

- *Personnel Risk Assessments* – PJM should continue to enhance its processes and procedures for documenting and tracking personnel risk assessments (PRAs) because PJM's method of tracking PRAs contained manual processes that led to three instances in which the wrong PRA dates were entered into PJM's tracking system. While these errors did not result in violations of the Reliability Standards, the manual processes created the potential for PJM to untimely update PRAs, which could lead to violations of CIP Standard requirements and potential risks to security.

- *Inventory of Software within the Electronic Security Perimeter* – PJM needs to improve its ability to track software on its CAs within its Electronic Security Perimeters (ESPs) because PJM's procedures did not capture some of the

[2] Reliability*First* and SERC each define BES for assets within its footprint.

[3] Access is the ability to use, manipulate, modify, or affect an object, and can be broken into two categories: physical or logical. Logical access is achieved through the use of technology in computer information systems to access an object without being physically present within the object, such as through a network. Physical access requires a physical presence within the object.

supporting software packages that were installed as part of the main software package.[4]

- *Electronic Security Perimeter Access Points* – PJM's processes for conducting port scans of both its ESP access points and the CCAs within the ESPs should be enhanced to ensure PJM remains aware of all ports that may be enabled (i.e., open). Such enhancements will increase PJM's performance in this area, allowing PJM more effectively to ensure only necessary ports and services are open and to prevent unauthorized access to CCAs.

- *Change Control and Configuration Management* – PJM needs to enhance its processes and procedures governing its change control and configuration management (CCCM) to ensure all PJM employees properly follow them. PJM should enhance its preventative measures to emphasize the importance of following the CCCM processes and procedures, and preventing unauthorized changes to its systems.

- *Planning and Operating Models* – PJM should enhance its policies and procedures governing its planning and operating models to minimize inaccuracies and inconsistencies by: (1) improving its procedures for developing and validating its planning models to ensure all significant changes made to elements of the PJM system are reflected in the models; and (2) developing documented procedures for validating and benchmarking the performance of its operating models to ensure consistency in the model data between PJM and its Transmission Owners (TOs).

- *Plan to Continue Reliability Operations* – PJM should update its contingency plan to include: (1) a list of the critical transmission facilities to be monitored; (2) procedures and responsibilities for conducting annual tests of the plan; (3) procedures and responsibilities for providing annual training to implement the plan; (4) procedures for managing System Operating Limits (SOLs) and Interconnection Reliability Operating Limits (IROLs); (5) procedures for performing congestion management and generation dispatch; and (6) procedures for continuing reliability operations in the event a TO without a fully functioning backup control center has its primary control center become inoperable.

[4] An ESP is a layer of security acting as an electronic "fence" to control access to CCAs. Once an ESP is established, all cyber assets (whether they are designated as critical or not) within the fence must be known and protected as if they were critical in order to ensure that the actual CCAs remain protected.

2. Other Matters

We identified three areas of interest that are summarized below:

- *System Operating Limits* – Audit staff understands that PJM monitors and has operational responsibility for the facilities in its footprint rated below 230 kV. PJM performs these responsibilities pursuant to thermal limits and associated facility ratings, even though PJM excludes such facilities in its definition of SOL in its operations horizon.[5] Audit staff believes that PJM should strengthen its performance by defining SOLs consistently for the entire BES, and not just for facilities rated at 230 kV and above. Therefore, PJM should define SOLs for BES facilities rated at least from the 100 kV level. This practice would enhance PJM's ability to track and analyze SOL exceedances, and would increase transparency through PJM reports involving SOL exceedances, where applicable, to NERC and its Compliance Enforcement Authorities (Reliability*First* and SERC).

- *Interconnection Reliability Operating Limits* – Audit staff understands that PJM establishes, continually monitors, and takes appropriate actions to prevent exceedances of IROLs on the BES within its footprint in order to minimize the risk of cascading outages, instability, or uncontrolled separation that may otherwise occur. However, audit staff believes PJM should strengthen its own performance and the performance of its member TOs by enhancing the policies, procedures, and controls governing IROL exceedances to demonstrate the collective ability to prevent adverse effects on the system and to respond to exceedances within the maximum 30 minutes required by the Reliability Standards.

- *Compliance Enforcement for the Transmission Operator Function* – PJM, with one exception, is registered as the sole Transmission Operator (TOP) for the BES transmission facilities within its footprint.[6] PJM carries out its TOP functions through assignment of particular TOP tasks to its member TOs. Audit staff believes that PJM should continue to strengthen the clarity of the identity of the entity responsible for performing specific TOP tasks in order to: (1) ensure there are no gaps or unnecessary overlaps in the performance of TOP tasks; (2) ensure all entities are aware of their assigned duties with respect to

[5] The operations horizon covers the period from real-time operations up to one year in the future. The period extending beyond one year to a maximum of ten years is considered the planning horizon.

[6] American Electric Power Co., Inc. (AEP) is concurrently registered with PJM as a TOP, with AEP responsible for its facilities rated at 138 kV and below. *See* PJM Manual 03 section 1.2 at p. 8 (Rev. 39, 2011) (PJM Manual 03).

compliance with the Reliability Standards; and (3) better enable Reliability*First* and SERC, the Compliance Enforcement Authorities (CEAs) for TOPs and TOs in PJM's footprint, to administer the NERC Compliance Monitoring and Enforcement Program (CMEP) as it relates to PJM and its member TOs.

3. Recommendations

This section summarizes audit staff's recommendations to the audit's findings. Detailed recommendations are included in section IV of this report. Audit staff recommends that PJM adopt the following recommendations to address this report's audit findings:

1. Revise its processes of identifying CCAs to incorporate all of the suggested guidance issued by NERC.

2. Expedite the development and implementation of an automated, centralized process for managing logical access rights to CCAs that includes controls to address the concerns identified in the audit.

3. Strengthen its policies and procedures going forward to include requirements that all account access changes be communicated to responsible parties so that these parties are aware what access changes have been made, and are required to verify that each change is appropriate.

4. Revise its policies and procedures to assign reasonable expiration dates to transferred employees' old logical access rights and to require periodic action to extend the access rights of such transferred employees. If access is needed beyond the initially assigned expiration date, PJM's policies should, at a minimum, permit an extension only by prompting required action on the part of the responsible party.

5. Consider migrating to an automated system for processing PRAs. PJM should assess whether it is beneficial to automate the transfer of hire dates and PRA dates from its Human Resources system to its security training tracking system through the use of database technology.

6. Implement (if PJM decides not to employ automated procedures for PRAs) processes and procedures to validate data manually entered into (1) its Human Resources system related to hire dates and PRA dates, and (2) its security training spreadsheet.

7. Perform an inventory of software installed on each asset within its ESPs using all available tools and controls to develop a baseline inventory of software.

8. Strengthen its configuration management process, including enhanced procedures for conducting periodic reviews of assets within PJM's ESPs, to ensure PJM maintains an accurate inventory of installed software on all such assets.

9. Consider enhancing its policies and procedures for conducting port scans on its access points to the ESPs to verify comprehensively that only necessary ports and services are open.

10. Enhance its CCCM processes and procedures to include additional preventative measures to reinforce the importance of following these processes and procedures, such as providing additional training to relevant staff.

11. Continue to enhance its policies and procedures in place, including the implementation of PJM's automated software, to verify its planning models are current and consistent before using these models in PJM's planning activities.

12. Develop criteria and requirements for communicating information about significant changes on the PJM system between the TOs and PJM to ensure that these changes are reflected timely in PJM's Planning Models.

13. Develop a formal procedure to validate PJM's EMS Model and benchmark its performance to mutually agreed upon criteria in collaboration with TOs before deploying the EMS Model into use for real-time operations.

14. Update its contingency plan to include the list of critical transmission facilities and procedures for monitoring them.

15. Update its contingency plan to include a full list of systems/applications to be covered by the plan.

16. Update its contingency plan to include procedures and responsibilities for conducting annual tests of the plan and for providing annual training to implement the plan.

17. Develop procedures in its contingency plan for (1) manually managing SOLs and IROLs, and (2) performing manual congestion management and generation dispatch in the event both its control centers become inoperable.

18. Develop procedures in its contingency plan for continuing reliability operations in the event that a TO without a fully functioning backup control center has its primary control center become inoperable.

19. Continue its review of its SOL methodology, and define SOLs for BES facilities rated at least from the 100 kV level and above.

20. Keep NERC, the CEAs, and other parties informed of PJM's review of its SOL methodology and provide them the opportunity to participate in the review of the findings.

21. Develop procedures for documenting formal lessons-learned resulting from load-shedding drills that are communicated to all parties involved.

22. Review load-shedding drill results and update governing policies and procedures to reflect the performance demonstrated in these drills.

23. Enhance its policies and procedures to address scenarios involving IROLs with 15-minute load dump ratings.

24. Enhance its policies governing protective relay settings and associated IROLs to include procedures for operating above load dump ratings for the time required to take responsive action.

25. Continue to review and update the TOP Matrix, PJM manuals, and other necessary documents to clarify responsibility for, and performance of, reliability tasks and eliminate any gaps or unnecessary overlaps.

26. Coordinate its review in response to Recommendation 25 with NERC, the CEAs, and other parties to keep them informed of the process and provide them the opportunity to participate in the review.

27. Submit the results of its review in response to Recommendation 25 to the Division of Audits within 30 days after completion.

28. Coordinate with AEP to develop procedures for managing shared reliability risks that may require coordinated response to avoid potential reliability gaps or overlaps.

D. Compliance and Implementation of Recommendations

We further recommend that PJM:

- Submit for audit staff's review its plans for implementing this report's recommendations. PJM should provide these plans to audit staff within 30 days of the issuance of the final audit report in this docket.

- Submit quarterly reports to the Division of Audits describing PJM's progress in completing each action recommended in the final audit report. PJM should make these nonpublic quarterly filings no later than 30 days after the end of each calendar quarter, beginning with the first quarter after the final audit report is issued, and continuing until PJM completes all recommended corrective action.

- Submit copies of any written policies and procedures developed or modified in response to recommendations in the final audit report. These documents should be submitted for audit staff's review in the first nonpublic quarterly filing subsequent to PJM's completion of any such document.

II. PJM Reliability Operations

When Reliability Standards developed by NERC first became mandatory and enforceable within the United States on June 18, 2007, PJM registered with Reliability*First* and SERC as a TOP, Transmission Planner (TP), Reliability Coordinator (RC), Transmission Service Provider, Balancing Authority (BA), Planning Authority, and Resource Planner. In 2008, PJM registered as an Interchange Authority in the Reliability*First* and SERC regions.[7] As a registered TOP, BA, and RC, PJM became subject to CIP CMEP activities on July 1, 2008.

At the advent of the NERC Functional Model, PJM and most of its member TOs determined that PJM's designation as the regional transmission organization, and its attendant authorities and responsibilities, were best reflected in the functions assigned to an RC and TOP in the Functional Model. Therefore, PJM registered as the RC and TOP for its footprint. However, initially, some of the TOs within PJM's footprint also chose to register as TOPs, resulting in several concurrent TOP registrations. Over time, PJM and its member TOs determined that the PJM approach of acting as the sole TOP for the entire footprint to centralize the concept of command and control made the most sense, and all but one PJM member TO, AEP, de-registered from its TOP function, which was assumed by PJM. AEP remains the only concurrently registered TOP with PJM.[8]

While PJM is the registered TOP for TOs located within its footprint, it has chosen to assign the responsibility for the performance and demonstration of compliance with some reliability tasks associated with the TOP function to the TOs. PJM maintains a spreadsheet matrix (TOP Matrix) to track the reliability responsibilities it shares with its member TOs as defined in PJM's Consolidated Transmission Owners Agreement (TOA) and Amended and Restated Operating Agreement (Operating Agreement), and other governing documents.[9] The TOP Matrix is intended to be a composite listing of the NERC Reliability Standard requirements that apply to the TO and TP functions. Simply

[7] The CEA duties for ensuring PJM's compliance with Reliability Standards are shared between Reliability*First* and SERC. For joint CMEP activities, Reliability*First* or SERC take the lead role based on the location of the facility(ies) involved. Regarding CMEP activities related to PJM, Reliability*First* takes the lead because most PJM-registered facilities fall within the Reliability*First* region.

[8] According to PJM, AEP's registration as a TOP is only for facilities rated at 138 kV and below.

[9] PJM established the TO/TOP Matrix v4 Task Force as a joint effort among the PJM Reliability Standards and Compliance Subcommittee, the Transmission Owners Agreement-Administrative Committee, and the Systems Operations Subcommittee – Transmission to review and update the TOP Matrix proactively.

put, the TOP Matrix is a cross-reference guide used to show where assigned reliability tasks are documented in the PJM agreements, manuals, and PJM Compliance Bulletins.

PJM has a seven-member Internal Audit department that conducts audits on subjects ranging from accounting and procurement controls to cyber security. The PJM Board of Directors has a three-member Audit Committee that oversees internal audits' performance and monitors PJM compliance with financial reporting rules, internal controls, and legal and regulatory requirements, including the NERC Reliability Standards. To address the reliability aspects of PJM's operations, PJM also has an eleven-member internal Regulatory Oversight and Compliance Committee (ROCC) that provides an enterprise-wide focus on compliance. The ROCC is responsible for managing all compliance efforts across the organization, including reviewing and reporting all compliance events, identifying and implementing compliance training, and identifying and adopting industry best practices. Incidents are referred to the ROCC if there is a reasonable possibility of potential noncompliance. The ROCC informs PJM's Chief Executive Officer and Board Governance Committee through monthly and situational reports on compliance activities.

During the audit period, PJM migrated to a new energy management system (EMS) to run its power grid and market systems. The new system, the Advanced Control Center (AC2), equipped PJM with two state-of-the-art synchronous control centers – each is fully functional and able to run the system independently if needed. The conversion to AC2 involved development and testing, including production simulations and mock migrations. Audit staff was mindful of the time and resources required of PJM staff for the successful migration to AC2 and did not schedule site visits or seek discovery during the period surrounding its "go live" date.

III. Introduction

A. Objectives

The audit objective was to evaluate PJM's performance as: (1) a Table 1 entity responsible for compliance with certain CIP Reliability Standards;[10] and (2) a TOP and TP. The audit covered the period from June 18, 2007, to July 18, 2012.

B. Scope and Methodology

This performance audit was undertaken to help PJM maximize its compliance with mandatory Reliability Standards and to point to areas where enhancements would result in improved effectiveness and efficiencies in PJM's performance and operations as a TOP, TP, and a Responsible Entity for the CIP-002 through CIP-009 Reliability Standards. Audit staff used a risk-based audit approach in examining PJM's performance with respect to cyber security and its operations and planning as a TOP and TP. The approach was focused not only on PJM's compliance with the Reliability Standards but on PJM's performance in the audited areas. Specifically, audit staff examined PJM's compliance with mandatory Reliability Standards, as well as evaluated the efficiency and effectiveness of PJM's processes, procedures, manuals, and other criteria that PJM followed to achieve compliance.

In accomplishing its audit work, audit staff interviewed many of PJM's subject matter experts when we reviewed and analyzed PJM's operations and performance. Audit staff points out that throughout the audit period PJM readily made its subject matter experts available to answer and address audit staff's questions and concerns. Audit staff interviewed more than 50 PJM subject matter experts, many of whom were interviewed multiple times, to discuss the audited areas and audit staff's concerns. These subject matter experts were open and transparent in their discussions with audit staff, which greatly assisted our testing and evaluations.

[10] Version 1 of the CIP-002 through CIP-009 Reliability Standards included an implementation plan that specified groups of entities (Table 1 entities, Table 2 entities, and Table 3 entities) and when entities in those groups needed to be "compliant" and "auditably compliant" with the CIP-002 through CIP-009 Reliability Standards, as reflected in NERC's Guidance for Enforcement of CIP Standards. PJM, as a Table 1 entity, was expected to have achieved "compliant" status, as defined in the Implementation Plan, for thirteen requirements in these CIP Standards by July 1, 2008. Registered entities that must comply with any of these standards generically are called Responsible Entities.

Throughout the audit, audit staff conferred with NERC, Reliability*First*, and SERC staffs. This process provided valuable information to audit staff, particularly given the roles of Reliability*First* and SERC as the CEAs for Reliability Standards applicable to PJM. This collaboration included, among other things, discussing PJM's reliability history and reviewing Reliability*First*'s and SERC's joint audits and spot checks of PJM, which assessed PJM's compliance with all applicable actively monitored requirements of the Reliability Standards.

To address overall audit objectives, audit staff performed the following:

- Identified the standards and criteria to be used to evaluate PJM's compliance with each issue within the audit scope, including Commission orders, the Reliability Standards, and NERC guidance documents;

- Reviewed publicly available materials, including PJM's filings in FERC's eLibrary and information available on PJM's web site;

- Issued data requests to gather information on PJM's organizational structure and the identification of key personnel; and

- Held numerous conference calls with PJM personnel, including subject matter experts as well as PJM's compliance and legal staff, to discuss the audit. These discussions ranged from data request clarifications to in-depth conversations about PJM's cyber security program and operations and planning activities.

Critical Infrastructure Protection (Order No. 706)

The CIP Reliability Standards, which the Commission initially approved in its Order No. 706, provide a cyber security framework for the identification and protection of "Critical Cyber Assets" to support the reliable operation of the Bulk-Power System.[11] In addition to the methodology above, to test PJM's compliance with and performance of these Reliability Standards, audit staff:

- Issued data requests to gather details regarding PJM's CIP compliance program, focusing on these areas:

    - Identification and management of PJM's CAs and CCAs;

[11] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040 at P 463, *order denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

- Controls over granting access to CAs and CCAs; and

- Management of logical access to CCAs, monitoring of CCAs, and CCA recovery plans.

- Conducted two site visits to PJM's headquarters in Valley Forge, PA. During the site visits, PJM provided to audit staff presentations focused on the major elements of PJM's cyber security program as well as the areas identified in the data requests. These presentations served as a framework for audit staff's interviews and open discussions with PJM personnel responsible for performing key tasks, including: (1) the human resources department responsible for managing personnel risk assessments; (2) the information technology and security department responsible for security monitoring, vulnerability assessments, and account access management; and (3) the compliance and legal departments responsible for overseeing the CIP program. In addition, PJM had other subject matter experts from various support departments on call in the event they could provide additional relevant information to facilitate the site visits. Throughout the site visits, PJM staff readily responded to onsite requests for information and clarification, and facilitated audit staff's sampling and review of numerous documents related to PJM's management and control of CAs and CCAs, and the associated access rights to them. Audit staff covered the following areas at PJM during the site visits:

  - Processes for conducting personnel risk assessments and background checks;

  - Methodology for determining CAs and CCAs, and its application;

  - Processes for granting, controlling, and tracking access to CAs and CCAs;

  - Processes for managing CCAs, including change control and configuration management, patch management and platform upgrades, cyber security policies, and recovery plans; and

  - Network, facilities, and communications architecture and diagrams.

Operations and Planning (Order No. 693)

The operations and planning Reliability Standards, which the Commission initially approved in Order No. 693, are also designed to support the reliable operation of the

Bulk-Power System.[12] In addition to the methodology above, to test PJM's compliance with and performance of these Reliability Standards as they apply to PJM as a registered TOP and TP, audit staff:

- Issued data requests for details regarding PJM's roles and responsibilities as a TOP and TP. Audit staff focused on these areas:
    - PJM's transition to, and registration under, the NERC Functional Model;
    - PJM's operations as a TOP and TP; and
    - The training and certification of system operators.
- Conducted a site visit to PJM's headquarters in Valley Forge, PA. Similar to the other site visits, PJM provided presentations focused on the areas audit staff identified in data requests and made numerous subject matter experts available for interviews and discussions, including system operators and staff from: (1) the operations department responsible for daily reliability operations; (2) the planning department responsible for conducting reliability assessments; (3) the training department responsible for managing operator training and certification; and (4) the compliance and legal departments responsible for assisting organizational compliance with the reliability standards. In addition, audit staff toured PJM's primary control center in multiple sessions, first in order to gain an understanding of daily operations and the tools and resources PJM utilizes to perform TOP and TP functions, and then, after interviews of PJM subject matter experts, to observe visually processes previously discussed verbally. Specifically, audit staff covered the following areas during the site visit:
    - PJM's registration as a TOP and TP;
    - The coordination between PJM and member TOs to perform TOP and TP functions;
    - The history and evolution of the PJM TOP Matrix;
    - PJM's processes for maintaining situational awareness over TOP operations;
    - Near-term and long-term planning assessments; and

[12] *Mandatory Reliability Standards for the Bulk-Power System*, Order No. 693, FERC Stats. & Regs. ¶ 31,242, *order on reh'g*, Order No. 693-A, 120 FERC ¶ 61,053 (2007)

  - Elements of system operator training and its evolution.

- Held a series of conference call discussions with PJM subject matter experts in lieu of a site visit to address audit staff's areas of concern and collaboratively discuss ways for PJM to improve its reliability operations. Specific areas audit staff discussed with PJM included:

  - PJM's application of SOL and IROL limits;

  - Coordination with TOs to ensure continuity of reliability operations;

  - Communication of outages and modifications of protection systems for the transmission facilities it operates;

  - Processes and procedures governing PJM's operating models and next-day scheduling;

  - Frequency response in the Eastern Interconnect dynamic model; and

  - Coordination with the TOs to evaluate long-term planning models.

IV. Findings and Recommendations

A. Performance Enhancements

1. Identifying Critical Cyber Assets Associated with Critical Assets

PJM's process for identifying CCAs associated with its CAs needs to be enhanced to ensure that all CCAs related to the reliability or operability of the BES are properly identified.[13] These enhancements will help PJM ensure no potential gaps exist in its process for identifying CCAs.

Pertinent Guidance

NERC Reliability Standard CIP-002-3 – Cyber Security – Critical Cyber Asset Identification

> R3. Critical Cyber Asset Identification – Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary.

NERC developed guidelines intended to inform the entities on the application of risk-based methodologies used under NERC Reliability Standard CIP-002-1 for identification of CAs.[14] NERC also developed guidelines intended to assist a Responsible Entity in identifying CCAs as described in CIP-002, R3.[15]

---

[13] Reliability*First* and SERC each define BES for assets within its footprint.

[14] Security Guideline for the Electricity Sector: Identifying Critical Assets (Nov. 19, 2009), *available at* http://www.nerc.com/fileUploads/File/Standards/Critcal_Asset_Identification_2009Nov19.pdf

[15] Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets (June 17, 2010), *available at* http://www.nerc.com/fileUploads/File/Standards/Critcal%20Cyber%20Asset_approved%20by%20CIPCl%20and%20SC%20for%20Posting%20with%20CIP-002-1,%20CIP-002-2,%20CIP-002-3.pdf.

In addition, NERC posted Frequently Asked Questions on Reliability Standard CIP-002 on its web site that states:

> [R]edundancy does not affect the criticality of any asset. Redundancy will only affect availability and reliability while not improving integrity or information confidentiality and may in fact increase the Cyber Asset's exposure to a cyber attack. For the purpose of security, each CCA and redundant CCA must be protected under the Cyber Security Standards as CCAs.[16]

Background

The process of identifying CCAs required during the audit period began with identifying assets critical to supporting the reliable operation of the BES using a risk-based assessment methodology (RBAM). Reliability Standard CIP-002-3, R3 lists categories of assets that must be considered in the assessment, including control centers and backup control centers. In Order No. 706, the Commission recognized the industry's need for additional guidance on developing RBAMs.[17] The Commission also recognized the need to take into account the individual circumstances of a responsible entity, and left it to NERC's discretion "whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two."[18]

In response to the Commission's concerns, NERC developed a guidance document entitled "Security Guideline for the Electricity Sector: Identifying Critical Assets" (CA Guideline). Audit staff points out that NERC only provided suggested guidance on this topic in order to address possible confusion in the industry, and did not make its suggestions prescriptive for all registered entities. NERC's CA Guideline: (1) defines which assets should be evaluated; (2) describes how CAs should be defined and describes special considerations for asset types; (3) defines evaluation guidance that could be used to determine if an asset is critical; (4) discusses listing the essential functions of the asset; and (5) discusses what should be documented and the criteria for determining whether an asset is critical. The CA Guideline indicates that a control center should be evaluated according to the guidance described in Section C, Table C-3. To supplement this guidance, NERC also developed an additional guidance document entitled "Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets" (CCA Guideline).

---

[16] Frequently Asked Questions for Cyber Security Standards (Mar. 2006), *available at* http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-002-1_FAQs_20090217.pdf.

[17] Order No. 706, 122 FERC ¶ 61,040 at P 238.

[18] *Id.* P 253.

The CCA Guideline expands upon the control center evaluation guidance in Section C of the CA Guideline.

The Commission's recent approval of Version 4 of the CIP Reliability Standards, which will become effective April 1, 2014, will eliminate the use of an RBAM.[19] Instead, Responsible Entities will use an approved list of criteria to specify each Responsible Entity's assets that must be considered critical.[20] Under Version 4, control centers and backup control centers used to perform the functional obligations of a Reliability Coordinator are considered CAs.[21] Despite these changes, Version 4 does not alter the process for identifying CCAs. NERC states that "[t]he Critical Cyber Assets reference document was developed in the context of Versions 1, 2, and 3, and is generally applicable to Version 4."[22]

PJM used NERC's guideline to modify its RBAM after a CIP audit conducted by Reliability*First* in February of 2010. PJM developed an RBAM for determining CAs and associated CCAs based upon the definition of Adequate Level of Reliability (ALR) outlined by NERC in its guidance documents. However, through discussions with PJM, audit staff found that PJM adopted only parts of the NERC guidance documents. Specifically, PJM did not utilize Table C-3 related to control centers, which describes typical control center systems and provides example criteria to be considered while determining the criticality of these systems when identifying its list of associated CCAs. The example criteria in Table C-3 correlate the types of functions that should be considered critical based on one or more of six BES characteristics that support ALR. As a result of PJM's decision not to utilize the full guidance NERC developed, audit staff expressed concern to PJM that it had not identified and classified all assets that perform functions critical to the reliability and operability of the BES as CCAs. Specifically, audit staff identified two assets that it believed were performing critical functions. While PJM did not agree the two assets should have been classified as CCAs, PJM has since addressed audit staff's concern as discussed below.

One of the assets identified by audit staff was a PJM system that monitors, controls, and schedules an aggregate of approximately 11,000 MW of generation. Each of the generating units associated with this system was rated 100 MW or less, and provided energy and ancillary services to the PJM Balancing Authority function. This system collects real-time status and meter information, and sends operating signals to

[19] *Version 4 Critical Infrastructure Protection Reliability Standards*, Order No. 761, 77 Fed. Reg. 24,594 (April 25, 2012), 139 FERC ¶ 61,058 (2012), *order denying clarification and reh'g*, 140 FERC ¶ 61,109 (2012).

[20] *Id.* P 22.

[21] *See id.* PP 48, 57.

[22] Standards: Reliability Standards. CIP-002-4 Cyber Security – Critical Cyber Asset Identification, *available at* http://www.nerc.com/page.php?cid=2|20.

small generating units. Although each generation unit on its own is small and can only have a minimal impact on the BES, the combined generation capacity of the units overseen by the system was approximately 11,000 MW. This amount of generation can have a significant impact on the BES, and because this system aggregates all of the units, audit staff believes the system performs a function essential to the operation of the BES.[23] In discussions with PJM about the system, PJM stated that the vast majority of the units controlled by this system are unregulated, the units are spread across PJM's footprint, and most of these units are renewable energy sources. However, audit staff notes that the type of generation a system controls or monitors is irrelevant to a determination of criticality under CIP-002-3, and when an asset used to perform a function essential to the operation of the BES is under cyber control, the associated asset should be designated as a CCA. Due to the combined capacity of the generation resources under the control of this system, audit staff believes that PJM should have identified it as a CCA.

The second system audit staff believes that PJM should have classified as a CCA was primarily used to calculate Area Control Error (ACE) for the PJM Balancing Authority and consisted of an Automatic Generation Control (AGC) system. In discussions with PJM about the system, PJM staff explained that it did not identify it as a CCA for two main reasons: (1) PJM has other means to perform the AGC function, as this system is a tertiary measure (i.e., a backup to a backup), and (2) the system can only provide AGC for half of its generation units in PJM's footprint (i.e., PJM-West node). However, NERC's document on Frequently Asked Questions for Reliability Standard CIP-002 clearly indicates that redundancy does not preclude an asset from being identified as critical. Audit staff believes that if an asset, regardless of whether it is tertiary or otherwise, fulfills a critical function, that asset should be designated as critical. Since this system has generator base point control and a full AGC suite, audit staff believes the system is a cyber asset that performs ACE calculations and AGC functions. Since these functions are essential to the operation of one or more control centers (which are CAs), audit staff believes PJM should have classified this system as a CCA.

PJM acknowledged that one of the systems is now considered a CCA as part of PJM's new Energy Management System (EMS), known as Advanced Control Center (AC2), when AC2 was brought online in the fourth quarter of 2011. Moreover, the other system is no longer used in the same manner as it was prior to AC2, as the critical functions it was capable of performing have been disabled.

Audit staff evaluated PJM's process of identifying CAs and associated CCAs in order to determine whether PJM's adoption of only parts of NERC's guidance creates any gaps or risks to system reliability, and whether PJM's CA and associated CCA

[23] The 11,000 MW represents approximately eight percent of PJM's peak demand for 2011 and is larger than the total amount of reserve PJM carried at any time during the audit period. Loss of ability to monitor and control this amount of generation represents a significant reliability risk.

identification process effectively identifies assets that are critical to system reliability and have associated cyber assets. Audit staff interviewed PJM personnel about its use of NERC's guidance and the use of ALR as a means for PJM's risk-based assessment of CAs and associated CCAs. PJM informed audit staff that at the time PJM was developing its methodology using ALR, NERC's CA Guideline was still a draft document. PJM decided to develop a "bright line" test to evaluate its CAs, meaning PJM established objective criteria that left little to no room for interpretation when identifying its CAs. During the following year's mandatory review of its RBAM, PJM again did not use Table C-3 guidance, stating that PJM never revisited NERC's guidance after it became effective to determine whether PJM should update its policy or change its methodology.

Audit staff's review of PJM's process for identifying CCAs revealed that this process could be improved to consider all assets capable of providing information used to make operational decisions regarding BES reliability, or providing control center functionality for aggregated BES assets critical to reliable BES operation. When PJM conducts an annual review of its lists of CCAs, PJM should review all relevant NERC guidance documents to determine whether PJM's processes follow the current recommendations.

Recommendations

We recommend that PJM:

1. Revise its processes of identifying CCAs to incorporate all of the suggested guidance issued by NERC.

2. Access to Critical Cyber Assets

PJM needs to improve its processes and procedures for managing employees' logical (i.e., electronic) access rights to CCAs for access changes and for terminating access rights of employees to CCAs.[24] PJM should improve its performance by eliminating its reliance on a decentralized, manual process for implementing change requests and removing employees' access rights to CCAs.

Pertinent Guidance

NERC Reliability Standard CIP-004-3 – Cyber Security – Security and Training

> R4. Access – The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

Background

Managing Change Requests

PJM had implemented a procedure to manage coordination of all requests for access to CCAs by use of an Account Authorization Team (AAT). In line with the industry best practice of separation of duties, this group did not request or approve access, nor did it implement the approved access changes. The AAT simply facilitated the implementation of approved access changes by acting as an intermediary between PJM managers requesting access for employees and the information technology (IT) personnel responsible for making access changes. The process involves an AAT member (and one not involved in the initial authorization request for access) reviewing the access change request and determining its appropriate implementation by use of the documentation of its completion (i.e., the emails from IT and the daily reconciliation reports).

In examining this process, audit staff noted instances in which confirmation emails sent by IT personnel representing that the change was complete did not have sufficient information to permit the AAT reviewer to know whether the change had actually been

[24] Access is the ability to use, manipulate, modify, or affect an object, and can be broken into two categories: physical or logical. Logical access is achieved through the use of technology in computer information systems to access an object without being physically present within the object, such as through a network. Physical access requires a physical presence within the object.

made appropriately. The confirmation emails from IT personnel simply stated that the requested change had been made, but provided no evidence of the change to the AAT. In addition, audit staff noted that the daily reconciliation reports upon which the AAT was relying to verify the appropriate implementation of the change request were not adequate to permit effective verification. These reports did not provide the level of granularity necessary to verify employees' specific electronic access rights at the permission level.

In addition, PJM's decentralized process of managing logical access meant that numerous daily reconciliations reports needed to be reviewed by the ATT, further increasing the inefficiencies of the process. Some of these reports showed account and role changes, but others showed only account additions and deletions. Without a consistent level of detail showing the permission-level access on the accounts, PJM's AAT was hampered in its ability to ensure accuracy in its management of authorized logical access to CCAs.

Terminating Access Rights

Audit staff's review also disclosed that PJM's process for terminating access rights of employees who had transferred to a new position within the company was not robust. Under the procedures in place during the audit period, transferred employees retained all access rights during the transition period to allow them to complete tasks and responsibilities under their old positions. Each quarter, PJM managers reviewed the physical and logical access lists and determined whether changes were needed, such as removing access for an employee who had completed the transition to a new position.

Audit staff believes that personnel should maintain access rights of their old position only for as long as the access is necessary for the performance of their ongoing duties. By maintaining these access privileges until management takes action to remove them, PJM potentially permitted transferred employees to retain access privileges they no longer needed. In Order No. 706, the Commission recognized that "there may be operational reasons that justify retention of access privileges after an employee transfers, but the default procedure should be to cancel access privileges at transfer and to document any exceptions to that policy for audit purposes." For this reason, audit staff believes that rather than allowing permissions to continue until revoked by the manager, the default should be to permit a limited transitional period for access, which would terminate at a date certain unless explicitly extended by the manager. This change would not only strengthen the access controls, but may also provide incentives for a more efficient transition of duties and responsibilities.

Summary

PJM's existing process for managing logical access to CCAs needs to be enhanced to address all potential compliance risks. PJM recognizes the inherent complexities and

risks involved in using a decentralized, manual process for access control. Over a year ago, PJM began implementing incremental steps to improve in this area. PJM has begun to move toward an automated, role-based access process with a centralized management tool, which will ease the complexity of managing hundreds of accounts with varying degrees of access rights. However, to date this process has not been fully implemented, and the manual process currently in place could result in compliance risks and potential risks to the BES. To address these risks, PJM must strengthen and revise its existing policies and procedures, as well as implement fully its automated centralized process for managing logical access rights to CCAs.

Recommendations

We recommend that PJM:

2. Expedite the development and implementation of an automated, centralized process for managing logical access rights to CCAs that includes controls to address the concerns identified in the audit.

3. Strengthen its policies and procedures going forward to include requirements that all account access changes be communicated to responsible parties so that these parties are aware what access changes have been made, and are required to verify that each change is appropriate.

4. Revise its policies and procedures to assign reasonable expiration dates to transferred employees' old logical access rights and to require periodic action to extend the access rights of such transferred employees. If access is needed beyond the initially assigned expiration date, PJM's policies should, at a minimum, permit an extension only by prompting required action on the part of the responsible party.

3. Personnel Risk Assessments

PJM should continue to enhance its processes and procedures for documenting and tracking PRAs because PJM's method of tracking PRAs contained manual processes that led to three instances in which the wrong PRA dates were entered into PJM's tracking system. While these errors did not result in violations of the Reliability Standards, the manual processes created the potential for PJM to untimely update PRAs, which could lead to violations of CIP Standard requirements and potential risks to security.

Pertinent Guidance

NERC Reliability Standard CIP-004-03 – Cyber Security – Personnel and Training

> R3. Personnel Risk Assessment – the Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

The personnel risk assessment program shall at a minimum include:

> R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to collective bargaining unit agreements, depending upon the criticality of the position.
>
> R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
>
> R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004-3.

Background

PJM's process for ensuring compliance with Reliability Standard CIP-004-3 (PRA program) began with PJM requiring that a PRA be performed on every employee, regardless of whether that employee needs access to CCAs. Audit staff points out that this practice goes beyond the requirements of the Reliability Standards and, for an entity of the size and strategic importance of PJM, represents superior registered entity practice. As part of its PRA program, PJM completes PRAs for all new employees before their start dates and for all contractors before they perform services. PJM's Human Resources (HR) department is responsible for maintaining the PRA results in PJM's Human Resources Information System (HRIS) and ensuring compliance with the requirements. The HR department does so by entering the PRA completion date into the HRIS after receiving the results from PJM's vendor and, each month, manually cross-checking the HRIS for PRA dates that are approaching the seven-year PRA renewal period mandated by CIP-004-3, R3.2. The HR department initiates the renewal process several months ahead of the required renewal date. Audit staff found that all of these processes and procedures meet or exceed the requirements of the Reliability Standards.

Audit staff's review of PJM's methods for tracking PRAs revealed some areas for improvement to ensure effective and efficient operations. While PJM has implemented a number of checks and balances in its processes for tracking PRAs, these processes remain mostly manual. For example, PJM manually compares its Human Resources spreadsheet, which contains information such as the hire date and PRA date, with the security training spreadsheet, which contains information such as the hire date, orientation dates, and security training dates. This comparison is done monthly to reconcile the data and maintain documentation that all newly hired personnel receive security training prior to being granted access to CCAs and annual security training thereafter.

Audit staff is concerned that reliance on manual processes may create the potential for errors when entering data independently of a previously verified source. The potential for such data transfer errors was demonstrated in a random sample of 30 PRAs taken during the site visit from PJM's master spreadsheet containing a total of approximately 1,160 PRAs. Upon learning of the selected sample, PJM disclosed to audit staff that it had identified two erroneous PRA dates when reviewing the supporting documentation for the sampled PRAs. In addition, upon completion of its testing, audit staff identified an additional error, representing a total of three errors identified in the random sample of 30. While these three specific errors did not lead to any instances of missed PRAs, audit staff is concerned that these types of errors could lead to problems in the future. If the dates PJM had recorded for the PRA completions are incorrect, PJM is less likely to ensure that it conducts seven-year follow-up PRAs on an individual in a timely manner, as required by Reliability Standard CIP-004-3, R3.2. PJM's use of strong database linkages to ensure data consistency and accuracy (i.e., a single source of

verification) would reduce the likelihood of compliance violations and ensure a higher level of reliability.

Recommendations

We recommend that PJM:

5. Consider migrating to an automated system for processing PRAs. PJM should assess whether it is beneficial to automate the transfer of hire dates and PRA dates from its Human Resources system to its security training tracking system through the use of database technology.

6. Implement (if PJM decides not to employ automated procedures for PRAs) processes and procedures to validate data manually entered into (1) its Human Resources system related to hire dates and PRA dates, and (2) its security training spreadsheet.

4. Inventory of Software within the Electronic Security Perimeter

PJM needs to improve its ability to track software on assets within its ESPs because PJM's procedures did not capture some of the supporting software packages that were installed as part of the main software package.[25]

Pertinent Guidance

NERC Reliability Standard CIP-007-03 – Cyber Security – System Security Management

> R3. Security Patch Management – The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> R3.1 The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
>
> R3.2 The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

Background

PJM implemented a security patch management program designed to timely identify new software vulnerabilities and the corresponding security patches and upgrades that have been released for the software residing within PJM's ESPs. Essential to this program was PJM's software configuration management process, during which PJM identified and documented a list of all software that resided within PJM's ESPs. Using this list, PJM then implemented its security patch management program that included several complementary approaches to identifying the security patches and upgrades available for each piece of software within PJM's ESPs. First, PJM relied on a

[25] An ESP is a layer of security acting as an electronic "fence" to control access to CCAs. Once an ESP is established, all cyber assets (whether they are designated as critical or not) within the fence must be known and protected as if they were critical in order to ensure that the actual CCAs remain protected.

subscription to a third-party alerting service to monitor and identify new vulnerabilities and the release of corresponding security patches and security upgrades. Additionally, PJM assigned particular security analysts to monitor a secondary source, such as vendor notification lists or a secondary third party service, to supplement the primary third-party service's efforts to identify new patches and upgrades.

In responding to audit staff's data requests, PJM disclosed to audit staff that it discovered its configuration management processes did not identify six software products residing on assets within its ESPs. PJM staff explained that its methods for creating and maintaining an inventory of software within its ESPs were not as comprehensive as they could be. PJM has enhanced its procedures to include the use of additional tools and layers of employee review. These enhancements will assist PJM in identifying all software and associated security patches and upgrades that reside within the ESPs.

Recommendations

We recommend that PJM:

7. Perform an inventory of software installed on each asset within its ESPs using all available tools and controls to develop a baseline inventory of software.

8. Strengthen its configuration management process, including enhanced procedures for conducting periodic reviews of assets within PJM's ESPs, to ensure PJM maintains an accurate inventory of installed software on all such assets.

5. Electronic Security Perimeter Access Points

PJM's processes for conducting port scans of both its ESP access points and the CCAs within the ESPs should be enhanced to ensure PJM remains aware of all ports that may be enabled (i.e., open). Such enhancements will increase PJM's performance in this area, allowing PJM more effectively to ensure only necessary ports and services are open, and to prevent unauthorized access to CCAs.

Pertinent Guidance

NERC Reliability Standard CIP-005-3 – Cyber Security – Electronic Security Perimeter(s)

> R2. Electronic Access Controls – The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s). . .
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter. . . .
>
> R4. Cyber Vulnerability Assessment – The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following: . . .
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled.

NERC Reliability Standard CIP-007-3 – Cyber Security – Systems Security Management

> R2. Ports and Services – The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

In summary, these CIP Reliability Standards require that an entity enable only necessary ports and services for CCAs and access points, have a process to ensure only necessary ports and services are enabled for CCAs, and verify that only the necessary ports and services are enabled for CCAs and access points.

Background

The purpose of an ESP is to logically segregate CCAs from the rest of the Responsible Entity's network to control and monitor traffic at the boundary of the perimeter as a layer of defense for network-based attacks. Access points to the ESP are the places where electronic traffic crosses its boundary of the ESP, and ports are the electronic doorways through which electronic traffic flows. To control access to the ESP, Reliability Standard CIP-005-3 mandates that only ports and services required for operations and for monitoring assets within the ESP be open. To ensure only the required ports and services are open, an entity must first know which ports are open and which services are running. Unauthorized open ports are vulnerabilities that may allow an attacker access to the assets within the ESP. Port scanning utilizes software applications to discover which ports are open. Performing regular port scans ensures that no unauthorized ports have been opened.

PJM scans both its ESP access points and the CCAs within its ESPs to ensure that only necessary ports and services are open. However, this method of scanning may not provide a complete picture of which ports are open, which could lead some PJM ports to be open but not visible to PJM through its current scans.

Audit staff expressed concern that PJM may not have a complete picture of which ports and services are open through its current method of scanning, and therefore PJM may not ensure effectively that only the necessary ports and services are open. PJM responded that it ensures only necessary ports and services are open at access points to ESPs through its policies and procedures. PJM users must request that a particular port or service be added to the authorized list of ports and services, and the request must go through an authorization and validation process prior to implementation. PJM also reviews the requested change as part of an annual validation process, which includes firewall configuration verification. While audit staff is encouraged by PJM's existing policies and procedures in place for accessing ports and services, PJM can benefit from enhancing these procedures to verify comprehensively that only necessary ports and services are open. Such enhancements will increase PJM's performance in this area, allowing PJM to achieve more effective awareness of all potential vulnerabilities and prevent unauthorized access to its ESPs.

Recommendations

We recommend that PJM:

9. Consider enhancing its policies and procedures for conducting port scans on its access points to the ESPs to verify comprehensively that only necessary ports and services are open.

6. Change Control and Configuration Management

PJM needs to enhance its processes and procedures governing its CCCM to ensure all PJM employees properly follow them. PJM should enhance its preventative measures to emphasize the importance of following the CCCM processes and procedures and preventing unauthorized changes to its systems.

Pertinent Guidance

NERC Reliability Standard CIP-003-3 – Cyber Security – Security Management Controls

> R6. Change Control and Configuration Management – The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

Background

CCCM is an important internal control for preserving the integrity and stability of an entity's information systems. Adequate CCCM processes and procedures allow an entity to document its system and control any changes to the system, ensuring that unplanned or unauthorized changes do not happen and that planned changes are well-managed. For example, CCCM procedures usually require management approval of changes, and an evaluation of whether the change is justified and how the change is expected to affect the information system.

PJM has developed and implemented strong processes and procedures documenting its CCCM. However, PJM did not perform its CCCM procedures adequately when PJM employees did not adhere to its processes and procedures. PJM disclosed to audit staff that during routine change reconciliation activities, it found several instances of unauthorized changes to its systems that resulted from employees not properly following the CCCM processes and procedures. Two of these incidents involved cyber assets not identified as CCAs nor used in the access, control and/or monitoring of the ESPs. However, the third incident involved a non-CCA that was used

in monitoring of PJM's ESPs.[26] While audit staff commends PJM for its diligence in identifying and disclosing these unauthorized changes, audit staff is concerned that (1) PJM employees did not follow company processes and procedures, and (2) the third incident involved a cyber asset that is not a CCA that was used in monitoring PJM's ESPs.

In discussions with audit staff about the third incident, PJM staff explained that it discovered changes that had been made to the cyber asset without being authorized through PJM's CCCM processes and procedures, bypassing the CCCM change controls, and therefore were unauthorized. These are limited instances; however, audit staff believes that PJM needs to improve its practices to ensure its CCCM procedures are followed and to maximize compliance with all applicable CIP standards in this area.

PJM staff acknowledged the importance of its CCCM processes and procedures and ensuring that PJM employees effectively follow them. To improve in this area, PJM has enhanced its controls to include additional reconciliation activities to identify instances of unauthorized changes to PJM's system. Audit staff also believes that PJM should enhance its preventative measures, such as additional employee training, to reinforce the importance of adhering to the CCCM processes and procedures.

Recommendations

We recommend that PJM:

10. Enhance its CCCM processes and procedures to include additional preventative measures to reinforce the importance of following these processes and procedures, such as providing additional training to relevant staff.

[26] Reliability Standard CIP-005-3a, Requirement R1.5 provides that cyber assets that are used to monitor ESPs, and the CAs and CCAs contained therein, must be afforded the same protection as CCAs.

7. Planning and Operating Models

PJM should enhance its policies and procedures governing its planning and operating models to minimize inaccuracies and inconsistencies by:

- Improving its procedures for developing and validating its planning models to ensure all significant changes made to elements of the PJM system are reflected in the models; and

- Developing documented procedures for validating and benchmarking the performance of its operating models to ensure consistency in the model data between PJM and its TOs.

Pertinent Guidance

In Order No. 693, the Commission explained that the Transmission Planning group of Reliability Standards is intended to ensure the Bulk-Power System is appropriately planned and designed to meet appropriate reliability criteria. The Commission stated that:

> Transmission planning is a process that involves a number of stages including developing a model of the Bulk-Power System, using this model to assess the performance of the system for a range of operating conditions and contingencies, determining those operating conditions and contingencies that have an undesirable reliability impact, identifying the nature of potential options, and the need to develop and evaluate a range of solutions and selecting the preferred solution, taking into account the time needed to place the solution in service. The proposed TPL Reliability Standards address: (1) the types of simulations and assessments that must be performed to ensure that reliable systems are developed to meet present and future system needs and (2) the information required to assess regional compliance with planning criteria and for self-assessment of regional reliability.[27]

The Commission further explained in Order No. 693 that Reliability Standard TOP-002 is intended to ensure that resources and operational plans, including those used in modeling, are in place to enable system operators to maintain the Bulk-Power System in a reliable state.[28] NERC Reliability Standard TOP-002-2b states that:

> R19. Each Balancing Authority and Transmission Operator shall

[27] Order No. 693, FERC Stats. & Regs. ¶ 31,242 at P 1683.
[28] *Id.* at P 1590.

maintain accurate computer models utilized for analyzing and planning system operations.

Background

Planning Models

As a regional transmission organization (RTO) and a registered Transmission Planner, PJM is responsible for planning the enhancement and expansion of transmission capability in the PJM footprint. PJM accomplishes this through a Regional Transmission Expansion Planning (RTEP) process that is used to identify transmission system upgrades and enhancements to provide for the operational, economic and reliability requirements of PJM customers over a fifteen-year horizon. As part of the RTEP process, PJM develops and runs planning models that span the planning horizon (e.g., near-term and long-term) that PJM uses to help identify enhancements to the system.

During discussions of the RTEP process, PJM staff explained that it begins each annual RTEP cycle by updating the base cases for its analyses using the latest data available from the Multiregional Modeling Working Group (MMWG). The MMWG collects data from various sources, including TOs, and develops base cases for the entire PJM region. In developing the 2009 RTEP, PJM used a 2008 series MMWG case as a starting point. However, PJM informed audit staff that the 2008 and 2009 MMWG case inadvertently did not reflect the actual impedance of a particular line that PJM staff had updated in the 2007 RTEP case in response to a change made by a TO. As a result, a significantly different line impedance was used for a major line in the PJM system, introducing an error to PJM's 2008 and 2009 RTEP cases. This error was not detected until PJM began the 2010 RTEP cycle, when a PJM stakeholder informed PJM that the error existed in the base case. Once it received notice of this error, PJM retooled its analyses using the updated impedance and informed the MMWG of the error so that the error would be corrected in MMWG cases. Audit staff believes that PJM's actions in quickly acknowledging the error and the need to correct it in the applicable modeling are commendable.

PJM explained that the update its staff made to the line impedance in 2007 was not reflected in the 2008 and 2009 MMWG base cases because a TO had not submitted updated model data to the MMWG that reflected the impedance change. PJM did not identify the error prior to using the MMWG base cases for its RTEP in 2008 and 2009. Audit staff is concerned that, while PJM staff was aware of the change in the line's impedance, it did not validate that this change was reflected in MMWG base cases prior to using them in the RTEP processes. PJM staff publicly acknowledged the need for improvement in this area and took the initiative to improve its procedures for ensuring its planning models are accurate. To this end PJM proactively implemented a policy governing modeling data used in the RTEP process on September 15, 2011 that included policies and procedures for the creation and verification of power system modeling data.

In discussions with PJM about further improvement to its RTEP process, audit staff acknowledged that given the substantial number of changes that are made to the various data elements contained in the TOs' models, it is a complex task for PJM to coordinate with the TOs and to validate each data element before beginning the RTEP process. However, PJM and audit staff agreed that the implementation of additional controls and reviews would further decrease the likelihood of introducing another error into the planning models. To accomplish this, PJM has developed several documented procedures, desk references, and automated tools that PJM staff now uses to validate planning models before they are used in the planning process. In addition, at the completion of audit fieldwork PJM staff explained that it was further improving its processes by developing a single piece of software that will automate each validation technique used by PJM staff so that errors do not propagate to the planning models used in the RTEP process. Audit staff is encouraged by these steps and believes PJM should continue to enhance its processes, procedures, and controls in this area.

Operating Models

PJM develops and operates a Real-Time Reliability Model (Energy Management System Model) that resides on PJM's Energy Management System (EMS). This model represents the power system facilities in the PJM footprint and relevant facilities interconnected to the PJM system, and is used to monitor the PJM system in real-time. This model is also used as a basis for PJM's calculation of real-time Locational Marginal Prices and, in conjunction with PJM's generation dispatch system that is used for modeling all PJM generating units, the models' results are used to control generation and assess economic and secure operating points for the electric system (collectively referred to as Operating Models). These Operating Models are created and maintained from input data PJM receives from various sources including TOs, Generation Owners, Load Serving Entities, and adjacent Reliability Coordinators.

As explained by PJM, there are instances in which PJM's Operating Models produce results that differ from results of models of a given TO. These inconsistencies can occur for a number of reasons, and PJM and the TOs strive to minimize these inconsistencies. To identify and understand the cause of the inconsistencies, PJM has developed various policies and procedures for PJM and TO staff to coordinate their analytical efforts during real-time once an operator has observed an inconsistency. While these policies and procedures are strong and appear to be adequate to resolve any discrepancies that may arise in real-time, audit staff believes that PJM should expand its policies and procedures to include additional steps for identifying and resolving any discrepancies before PJM deploys its Operating Models into real-time operations.

In discussions with PJM about the steps it has taken to ensure the accuracy of the data used in its Operating Models, PJM staff stated that it has outlined the various

requirements, processes, and controls that member TOs must follow in the modeling processes. In addition, PJM and its members have created a subcommittee to ensure all parties are fully aware and engaged in the modeling processes, as outlined in PJM's operating manuals. However, PJM did not have a formalized process for validating the model data submitted by the TOs or for benchmarking the performance of its EMS Model. PJM staff explained that it conducts ad hoc checks and reviews of data in place, but these controls have not been formalized. Audit staff believes that to minimize inconsistencies between the results of PJM and TO analyses, as well as to maximize performance in this area, PJM should formalize its process for validating its EMS Model and benchmark the model's performance to mutually agreed upon criteria in collaboration with TOs before being used in PJM's operations.

Recommendations

We recommend that PJM:

11. Continue to enhance its policies and procedures in place, including the implementation of PJM's automated software, to verify its planning models are current and consistent before using these models in PJM's planning activities.

12. Develop criteria and requirements for communicating information about significant changes on the PJM system between the TOs and PJM to ensure that these changes are reflected timely in PJM's Planning Models.

13. Develop a formal procedure to validate PJM's EMS Model and benchmark its performance to mutually agreed upon criteria in collaboration with TOs before deploying the EMS Model into use for real-time operations.

8. Plan to Continue Reliability Operations

PJM should update its contingency plan to include: (1) a list of the critical transmission facilities to be monitored; (2) procedures and responsibilities for conducting annual tests of the plan; (3) procedures and responsibilities for providing annual training to implement the plan; (4) procedures for managing SOLs and IROLs; (5) procedures for performing congestion management and generation dispatch; and (6) procedures for continuing reliability operations in the event a TO without a fully functioning backup control center has its primary control center become inoperable.

Pertinent Guidance

The Commission has made clear that, in the context of an Independent System Operator (ISO) or RTO, local control centers (LCCs) are part of the TOP function and expressed concern that they may be overlooked and not treated as such. The Commission provided guidance on this matter in Order No. 693, stating that:

> [I]n the context of an ISO or RTO or any organization that pools resources, decision-making and implementation are performed by separate groups. The ISO or RTO typically makes decisions for the transmission operator and, to a lesser extent, the generation operator, while actual implementation is performed by either local transmission control centers or independent generation control centers. The NOPR proposed that "all control centers and organizations that are necessary for the actual implementation of the decisions or are needed for operation and maintenance made by the ISO or RTO or the pooled resource organization are **part of the transmission or generation operator function in the Functional Model**." [Emphasis added and footnotes deleted.] [29]

Paragraph 142 of Order No. 693 further states that:

> The Commission's concern is that, particularly in the ISO, RTO and pooled resource context, there should be neither unintended redundancy nor gaps for responsibilities within a function. In particular, the Commission is concerned that such "gaps" could occur in the context of several Reliability Standards addressing matters related to activities other than directing or implementing real-time operations.[30]

[29] *Id*. P 130.
[30] *Id*. P 142.

The above paragraph from Order No. 693 lists in a footnote a number of such Reliability Standards where "gaps" could occur, including EOP-008 – Plans for Loss of Control Center Functionality.[31] NERC Reliability Standard EOP-008-0, R1 states that:

> Each Reliability Coordinator, Transmission Operator and Balancing Authority shall have a plan to continue reliability operations in the event its control center becomes inoperable. The contingency plan must meet the following requirements:
>
> > R1.1. The contingency plan shall not rely on data or voice communication from the primary control facility to be viable.
> > R1.2. The plan shall include procedures and responsibilities for providing basic tie line control and procedures and for maintaining the status of all inter-area schedules, such that there is an hourly accounting of all schedules.
> > R1.3. The contingency plan must address monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events. The plan shall list the critical facilities.
> > R1.4. The plan shall include procedures and responsibilities for maintaining basic voice communication capabilities with other areas.
> > R1.5. The plan shall include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan.
> > R1.6. The plan shall include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans.
> > R1.7. The plan shall be reviewed and updated annually.
> > R1.8. Interim provisions must be included if it is expected to take more than one hour to implement the contingency plan for loss of primary control facility.

Background

PJM is a NERC-registered TOP in the Reliability*First* and SERC regions. To perform its duties as a TOP, PJM has assigned some TOP responsibilities to member TOs and has required them to perform certain tasks through a coordinated approach with PJM to effectively operate the transmission system in PJM's footprint. As a TOP, PJM has developed contingency plans that outline the procedures, responsibilities, and actions to

[31] *Id*. n. 74.

be taken in the event of various emergencies, including the total loss of PJM's control center functionality. To prepare for this occurrence, PJM has developed a contingency plan that relies, in part, on the contingency plans and associated actions of the TOs to be carried out effectively.

During the audit period PJM maintained an operating memo that served as PJM's primary document for its contingency plan for loss of its control center. The memo included references to various operating manuals that outline the detailed steps and requirements associated with the contingency plan. This plan was specific to PJM's loss of control center functionality and did not include the procedures, responsibilities, and actions to be taken in the event a member TO's control center became inoperable. Because PJM relies on the TOs to perform some of its TOP functions, the TO control centers are essential to PJM maintaining reliability operations. Therefore, PJM has outlined the responsibilities related to each TO's plan for loss of its control center functionality that are required by Reliability Standard EOP-008-0 in PJM manuals and the TOP Matrix.

PJM validated each TO contingency plan primarily by reviewing it during routine audits of the TO and annual submission requirements and attestations as to the contingency plan's viability. In addition, Reliability*First* has recently begun auditing the TOs for their performance of TOP tasks, including those tasks assigned under EOP-008-0 related to contingency plans.

Audit staff's review of PJM's contingency plan revealed some areas for improvement. In particular, audit staff noted that PJM's operating memo that serves as the primary document for PJM's contingency plan did not include:

- A list of the critical transmission facilities to be monitored;
- A complete list of PJM's systems/applications to be covered by the plan;
- Procedures and responsibilities for conducting annual tests of the plan; and
- Procedures and responsibilities for providing annual training to implement the plan.

While some of these elements were outlined in other PJM documents, such as PJM operating manuals and PJM's web site, PJM did not integrate these elements or refer to other documents in which they were presented as part of the documentation of PJM's contingency plan. In addition, as part of its contingency plan, PJM stated that in the event of a complete loss of its generation dispatch function (i.e., the loss of control center operability) it would manage the system's IROLs and SOLs and perform congestion management manually. However, audit staff notes that PJM's contingency plan did not

include operating and testing procedures for this specific scenario, and believes PJM should enhance its documentation associated with the plan to ensure it has an effective plan for maintaining reliability operations.

In discussions with audit staff about its contingency plan, PJM stated that the TOs' plans add depth to PJM's redundancy and capability to continue reliability operations. PJM's contingency plan is based on evacuation to a redundant control room with a redundant EMS and voice/data communication facilities to maintain reliability operations. However, audit staff notes that at the commencement of the audit one significant TO in PJM's footprint did not have a functional backup control center, and another TO did not have a redundant state estimator. While the latter TO has since implemented a redundant state estimator at its backup control center, there is still one significant TO without a functional backup control center. Audit staff believes that PJM should enhance its contingency plan for loss of its control center and associated documentation to ensure it and the TOs, working together, can effectively maintain reliability operations.

During the course of the audit, PJM took additional steps to improve its plan. These improvements included: (1) developing and posting a list of PJM's critical monitored facilities; (2) adding details about its annual testing to ensure viability of the plan for loss of control center functionality, including the overall purpose and required results of the annual tests; (3) outlining annual training, including evacuation drills to ensure viability of the plan; and (4) referencing PJM's procedures for maintaining balancing operations, interchange management, and coordination with applicable entities. Audit staff is encouraged by these steps, and believes PJM should continue to work with the TOs to further improve the contingency plan for continuing reliability operations. Audit staff was also informed by PJM that efforts are underway by the TO that lacks a functional backup control center to address the issue of its backup control center and to implement interim procedures to supply PJM with data on critical facilities in the event that the primary control center becomes inoperable.

Recommendations

We recommend that PJM:

14. Update its contingency plan to include the list of critical transmission facilities and procedures for monitoring them.

15. Update its contingency plan to include a full list of systems/applications to be covered by the plan.

16. Update its contingency plan to include procedures and responsibilities for conducting annual tests of the plan and for providing annual training to implement the plan.

17. Develop procedures in its contingency plan for (1) manually managing SOLs and IROLs, and (2) performing manual congestion management and generation dispatch in the event both of its control centers become inoperable.

18. Develop procedures in its contingency plan for continuing reliability operations in the event that a TO without a fully functioning backup control center has its primary control center become inoperable.

Corrective Actions

During the course of audit fieldwork PJM made the following corrective actions to address audit staff's recommendations 14, 16, and 17:

1. Updated its contingency plan to include the list of critical transmission facilities and procedures for monitoring them.

2. Updated its contingency plan to include procedures and responsibilities for conducting annual tests of the plan and for providing annual training to implement the plan.

3. Developed procedures in its contingency plan for (1) manually managing SOLs and IROLs, and (2) performing manual congestion management and generation dispatch in the event both of its control centers become inoperable.

B. Other Matters

1. System Operating Limits

Audit staff understands that PJM monitors and has operational responsibility for the facilities in its footprint rated below 230 kV. PJM performs these responsibilities pursuant to thermal limits and associated facility ratings, even though PJM excludes such facilities in its definition of SOL in its operations horizon.[32] Audit staff believes that PJM should strengthen its performance by defining SOLs consistently for the entire BES, and not just for facilities rated at 230 kV and above. Therefore, PJM should define SOLs for BES facilities rated at least from the 100 kV level. This practice would enhance PJM's ability to track and analyze SOL exceedances, and would increase transparency through PJM reports involving SOL exceedances, where applicable, to NERC and its Compliance Enforcement Authorities (Reliability*First* and SERC).

Background

Operating to SOLs helps ensure that the BES remains stable even after the worst applicable contingency event occurs. Therefore, system operators plan and operate the system so as not to exceed these limits.

PJM's SOL definition does not include BES facilities rated at voltages below 230 kV. However, PJM represented that it operates the system respecting all limits on all monitored facilities, including all BES facilities. Specifically, PJM stated that it operates its system so that loadings on all PJM BES facilities are within normal ratings, and that immediately following any single contingency the loading on all remaining facilities can be expected to be within emergency ratings. Within 30 minutes of any malfunction or failure, PJM operators use the remaining facilities or procedures to restore conditions to a level within normal operating ratings.[33] PJM operators do this for all BES facilities, even those they do not designate as SOL facilities.

Audit staff understands that prior to 2009 PJM defined SOLs for all BES facilities in the PJM footprint. Audit staff is encouraged that PJM is actively taking steps to return to its previous SOL methodology, and that it had begun to consider whether there is a need to include facilities rated below 100 kV. Furthermore, PJM staff explained that it has held internal discussions regarding the FERC/NERC Staff Report on the 2011

[32] The operations horizon covers the period from real-time operations up to one year in the future. The period extending beyond one year to a maximum of ten years is considered the planning horizon.

[33] PJM Manual 3 section 2 (Rev. 40, Jun. 1, 2011).

Arizona – Southern California Blackout and its recommendations.[34] As a result of these discussions, PJM began exploring this issue with its member TOs. PJM initiated discussions on this issue with its Systems Operations Subcommittee in early June 2012. PJM also intends to hold discussions with operating personnel from its member TOs through its Markets and Reliability Committee and Operating Committee.

Recommendation

Audit staff believes that PJM is taking the right steps by reviewing its SOL methodology. This review could allow PJM to consistently apply this methodology to the entire BES within its footprint, not just to facilities rated at 230 kV and above. In addition, this review could also provide greater transparency surrounding SOL exceedances. These proactive steps taken by PJM should address audit staff concerns regarding SOL exceedances for facilities rated below the 230 kV level. Therefore, audit staff recommends that PJM:

19. Continue its review of its SOL methodology, and define SOLs for BES facilities rated at least from the 100 kV level and above.

20. Keep NERC, the CEAs, and other parties informed of PJM's review of its SOL methodology and provide them the opportunity to participate in the review of the findings.

[34] FERC/NERC Staff Report on the Arizona-Southern California Outages on September 8, 2011 (April 2012), *available at* http://www.ferc.gov/legal/staff-reports/04-27-2012-ferc-nerc-report.pdf.

2. Interconnection Reliability Operating Limit

Audit staff understands that PJM establishes, continually monitors, and takes appropriate actions to prevent exceedances of IROLs on the BES within its footprint in order to minimize the risk of cascading outages, instability, or uncontrolled separation that may otherwise occur. However, audit staff believes PJM should strengthen its own performance and the performance of its member TOs by enhancing the policies, procedures, and controls governing IROL exceedances to demonstrate the collective ability to prevent adverse effects on the system and to respond to exceedances within the maximum 30 minutes required by the Reliability Standards.

Pertinent Guidance

The NERC Glossary of Terms defines IROL as:

> A System Operating Limit that, if violated, could lead to instability, uncontrolled separation, or Cascading Outages that adversely impact the reliability of the Bulk Electric System.

NERC Reliability Standard TOP-007-0, R2 states:

> Following a Contingency or other event that results in an IROL violation, the Transmission Operator shall return its transmission system to within IROL as soon as possible, but not longer than 30 minutes.

The time to return a system to within an IROL if it is exceeded is denoted by Interconnection Reliability Operating Limit T_V (IROL T_V). The NERC Glossary of Terms defines IROL T_V as:

> The maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's T_V shall be less than or equal to 30 minutes.

NERC Reliability Standard PRC-023-1 – Transmission Relay Loadability requires that each TO, Generator Owner, and Distribution Provider "[s]et transmission line relays

so they do not operate at or below 115% of the highest seasonal 15-minute Facility Rating[35] of a circuit (expressed in amperes)."

PJM Manual 03 section 2.1.1 provides that: "[e]ach Transmission Owner must confirm that tripping should not occur when loaded at the load dump rating for at least 15 minutes."[36]

Background

An IROL is an operating limit that, if exceeded, may result in cascading outages, voltage instability, or uncontrolled separation that adversely impacts the interconnection and poses a serious threat to the system as a whole. PJM has established and continually monitors IROLs in its footprint, and has designed its policies, procedures, and controls to minimize the risk of exceeding an IROL beyond the time allowable by the Reliability Standards.

IROL Policies, Procedures, and Controls

Audit staff reviewed PJM's documents that govern the treatment of IROLs and held numerous discussions with PJM subject matter experts to understand how PJM implements IROL policies, procedures, and controls. Audit staff found that the majority of the IROLs defined by PJM on its system are based on ratings of equipment that, if operated at that rating, would afford system operators the 30 minutes to return the system below the IROL limit allowable under TOP-007-0. PJM has developed procedures that outline the steps to be taken and the responsibilities of PJM and its member TOs to coordinate and mitigate IROL exceedances within the allowable time. The final step in this process is for PJM to direct the TOs to shed load in order to return the system below the IROL limit.

PJM staff explained that it trains all system operators, including those of the TOs, on how and when to shed load in the event an IROL limit is exceeded. As part of this training, PJM routinely coordinates drills designed to simulate an actual PJM request to shed load. Audit staff notes that such training is a good practice and is important for identifying areas for improvement in implementation of the procedures as well as refining the procedures themselves. Audit staff reviewed and discussed the drills with PJM staff and discovered that TO operators are able to shed the required amount of load effectively, but not always in the prescribed timeframe outlined in PJM's procedures. Based on a review of the drill results, audit staff informed PJM that it is concerned that the

[35] When a 15-minute rating has been calculated and published for use in real-time operations, the 15-minute rating can be used to establish the loadability requirement for the protective relays.

[36] PJM Manual 03 section 2.1.1 at p. 23.

procedures followed by PJM and TO system operators will not enable them to shed load when an IROL is exceeded in the timeframe prescribed in the Reliability Standard. PJM responded that the drill results were discussed informally with its system operators and other relevant staff and the TOs. Audit staff believes that the drills and feedback communications are crucial to proper operation of the BES and encourages PJM to develop and document formal lessons learned from the drills and to report to all parties involved the strengths and weaknesses in performance. The parties involved should use this feedback as a means to improve performance in order to conduct the drill results and all of the necessary steps within the required timeframe. If performance in this area is not achieved, PJM should alter its procedures to ensure that it and its member TOs can respond within the required timeframe when an IROL is exceeded.

Through discussions with PJM staff, audit staff found that PJM has defined two IROLs in its footprint that are based on 15-minute thermal ratings of equipment (i.e., 15-minute load dump ratings) that, if operated at or potentially above those ratings, will afford system operators a maximum of only 15 minutes to return the system below the IROL limit. Audit staff expressed concern that PJM's procedures, as discussed above, which afford the operators 30 minutes to mitigate an IROL exceedance, may not be adequate to address these IROLs. PJM staff explained that these IROLs are rarely active, but that in the event of an actual exceedance of either IROL, PJM would take action with respect to this equipment within the 15-minute period to reflect the actual rating constraint. Audit staff notes that neither IROL was exceeded during the audit period. However, audit staff believes that PJM should enhance its existing written procedures to ensure that it could respond within the 30-minute window to exceedances of these two thermal IROLs. Also, PJM needs to ensure that TO operators are aware of these IROLs.

Audit staff also understood there is the potential for tripping of IROL facilities by their owners if an IROL is exceeded, which is dependent on the settings of the facilities' relays. If a facility relay is set to operate with a 15-minute rating in accordance with PRC-023-1, R1.2, such facility could be removed from service automatically if loading exceeds 115 percent of the load dump rating.[37] PJM Manual 03 section 2.1.1 provides that: "[e]ach Transmission Owner must confirm that tripping should not occur when loaded at the load dump rating for at least 15 minutes." However, the manual does not address the scenario of a facility loaded beyond 115 percent of its 15-minute rating, which could create a condition in which the PJM operator has no time to mitigate the exceedance. Audit staff is concerned that a TO's relays may trip a facility without allowing PJM operators time to mitigate an IROL exceedance.

[37] PRC-023-1, R1.2 requires relays to be set so they do not operate at or below 115 percent of the highest seasonal 15-minute Facility Rating.

Recommendations

We recommend that PJM:

21. Develop procedures for documenting formal lessons-learned resulting from load-shedding drills that are communicated to all parties involved.

22. Review load-shedding drill results and update governing policies and procedures to reflect the performance demonstrated in these drills.

23. Enhance its policies and procedures to address scenarios involving IROLs with 15-minute load dump ratings.

24. Enhance its policies governing protective relay settings and associated IROLs to include procedures for operating above load dump ratings for the time required to take responsive action.

3. Compliance Enforcement for the Transmission Operator Function

PJM, with one exception, is registered as the sole TOP for the BES transmission facilities within its footprint.[38] PJM carries out its TOP functions through assignment of particular TOP tasks to its member TOs. Audit staff believes that PJM should continue to strengthen the clarity of the identity of the entity responsible for performing specific TOP tasks in order to: (1) ensure there are no gaps or unnecessary overlaps in the performance of TOP tasks; (2) ensure all entities are aware of their assigned duties with respect to compliance with the Reliability Standards; and (3) better enable Reliability*First* and SERC, the CEAs for TOPs and TOs in PJM's footprint, to administer the NERC CMEP as it relates to PJM and its member TOs.

Pertinent Guidance

The Reliability*First* Organization Registration procedure explains that "[t]he purpose of the NERC Compliance Registry is to clearly identify those entities that are responsible for compliance to the NERC and Reliability*First* Reliability Standards."[39]

NERC developed a set of criteria by which to determine what entities must be registered if they perform specific reliability-related tasks. Regarding the TOP function, these criteria are as follow:

> III(d) Transmission Owner/Operator:
>
> III.d.1 An entity that owns/operates an integrated transmission Element associated with the Bulk Power System 100 kV and above, or lower voltage as defined by the Regional Entity necessary to provide for the Reliable Operation of the interconnected transmission grid; or
>
> III.d.2 An entity that owns/operates a transmission Element below 100 kV associated with a Facility that is included on a critical Facilities list that is defined by the Regional Entity.
>
> *[Exclusion: A Transmission Owner/Operator will not be registered based on these criteria if responsibilities for compliance with approved NERC Reliability Standards or*

[38] AEP is concurrently registered with PJM as a TOP, with AEP responsible for its facilities rated at 138 kV and below. *See* PJM Manual 03 section 1.2 at p. 8 (Rev. 39, 2011) (PJM Manual 03).

[39] Reliability*First* Organization Registration (Rev. 2, Apr. 1, 2011), *available at* https://www.rfirst.org/compliance/Pages/Organization%20Registration.aspx.

> *associated Requirements including reporting have been transferred by written agreement to another entity that has registered for the appropriate function for the transferred responsibilities, such as a Load-Serving Entity, generation and transmission cooperative or joint action agency as described in Sections 501 and 507 of the NERC Rules of Procedure.]*[40]

NERC Reliability Standard VAR-001-2, Voltage and Reactive Control

> R4. Each Transmission Operator shall specify a voltage or Reactive Power schedule at the interconnection between the generator facility and the Transmission Owner's facilities to be maintained by each generator. The Transmission Operator shall provide the voltage or Reactive Power schedule to the associated Generator Operator and direct the Generator Operator to comply with the schedule in automatic voltage control mode (AVR in service and controlling voltage).

NERC Reliability Standard PRC-001.1, System Protection Coordination

> R3.2 Each Transmission Operator shall coordinate all new protective systems and all protective system changes with neighboring Transmission Operators and Balancing Authorities.

Background

Prior to the implementation of mandatory Reliability Standards, PJM, as an RTO, had operational control of certain member TOs' transmission systems, including critical facilities rated down to, and in specific instances including elements of, the 69 kV system through the PJM Operating Agreement. This agreement required PJM member TOs to operate and maintain those transmission facilities per PJM's directives and manuals, and follow PJM operating instructions during an emergency.

When NERC became the ERO, it created a Functional Model that links responsible entities with associated reliability-related functions and respective tasks. As relevant here, PJM registered within the Reliability*First* and SERC regions as the TOP for its footprint and its member transmission owners registered as TOs, with one exception. AEP is registered as a TOP for its facilities rated at 138 kV and below.

[40] Appendix 5B: Statement of Compliance Registry Criteria, Revision 5.1, Effective January 31, 2012, *available at* http://www.nerc.com/files/Appendix_5B_RegistrationCriteria_20120131.pdf.

As a registered TOP for its footprint, PJM is required to comply with all Reliability Standards applicable to that function. To carry out the TOP function and comply with the TOP requirements, PJM has assigned responsibility for performing certain TOP tasks to the TOs in its footprint. These responsibilities are governed by the PJM TOA, Operating Agreement, and PJM operating manuals, which all PJM member TOs are required to follow. While PJM and its TOs have operated the system in this manner since long before Reliability Standards became mandatory in the United States, PJM's obligation to demonstrate compliance with TOP Reliability Standard requirements is a relatively new responsibility and requires significant coordination with its TOs and the CEAs.

PJM has developed a document termed the TOP Matrix that addresses Reliability Standard requirements that apply to the TOP function. This document is intended to "clarify the assignment of tasks based on the unique relationship between PJM and its Member TOs as defined in the TOA and Operating Agreement and described in detail in various PJM Manuals." [41] However, in discussions with PJM staff about the TOP Matrix and its use, audit staff found that the document does not establish or govern the TOP responsibilities assigned to the TOs; rather, it is simply a cross-reference guide to indicate where the assignment of various TOP tasks is documented in PJM's governing agreements and operating manuals. As such, the TOP Matrix is a "living document" that is constantly being reviewed and updated by PJM, the TOs, and the CEAs.[42]

To ensure PJM's compliance with the Reliability Standards applicable to a TOP, Reliability*First* adopted a practice of auditing the TOs, using the TOP Matrix, for compliance with TOP Reliability Standards.[43] Reliability*First* conducts these audits as an extension of its compliance audit of PJM as the TOP. However, in administering these audits there has been a lack of clarity of the identity of the entity responsible for performing specific tasks required by the TOP Reliability Standards. In part, the lack of clarity has arisen when the delineation of responsibilities in the TOP matrix differed from the specific language in the underlying operating agreements between PJM and a TO. When this situation arose, it was necessary for Reliability*First* to rely upon the operating agreements for determining compliance.

[41] http://pjm.com/committees-and-groups/task-forces/ttv4tf.aspx.

[42] Version 4 of the TOP Matrix is in use and Version 5 is being drafted.

[43] As stated above, the CEA duties for ensuring PJM's compliance with the applicable Reliability Standards are shared between Reliability*First* and SERC. For CMEP activities regarding PJM, Reliability*First* takes the lead because a greater percentage of PJM registered facilities are within the Reliability*First* region.

Audit staff determined that the PJM agreements, manuals, and procedures did not always clearly delineate between PJM and the TOs Reliability Standard responsibilities. This situation is understandable given that most of these PJM documents were drafted before the implementation of the NERC Functional Model and mandatory Reliability Standards. Audit staff notes that the CEAs responsible for administering the CMEP for PJM (i.e., Reliability*First* and SERC) agreed with audit staff that greater clarity in delineating responsibility for compliance with Reliability Standards among PJM and its member TOs would be beneficial. Audit staff identified three examples where increased clarity of the entity responsible for performing and demonstrating compliance for specific TOP tasks could be achieved: (1) communications of generator voltage schedules; (2) coordination of relay settings of facilities within PJM's footprint; and (3) PJM's coordination with AEP, which is concurrently registered for TOP responsibilities.

As to voltage schedules, Reliability Standard VAR-001-2, R4 requires a TOP to provide voltage or Reactive Power schedules to Generator Operators within the TOP's footprint.[44] PJM Manual 03 states that "PJM Transmission Owners may supply voltage schedules and a low and high bandwidth; however, Generation Owners [GO] who have not been provided a voltage schedule or a low and high bandwidth by a Transmission Owner are required to follow the PJM default voltage schedule[.]"[45] This language has led to confusion as to the registered entity that is responsible for providing a voltage schedule to GOs – PJM, as the TOP, or the relevant TO. Audit staff understands that Reliability*First* deems the default voltage schedule PJM provides to each GO to satisfy this Reliability Standard requirement. The confusion surrounding the assignment of the responsibility to provide such schedules arose from the statement in PJM Manual 03 that TOs "may supply voltage schedules" to GOs. PJM and the TOs are working on changing the TOP Matrix to resolve this issue.

Second, PJM's Manual 03 delegates to the PJM Relay Subcommittee the task of ensuring relay coordination between entities, a responsibility of the TOP function pursuant to Reliability Standard PRC-001.1, R3.2. However, PJM's Manual 03 does not require all TOs to participate in the subcommittee, potentially leading to a failure to ensure proper coordination of relays across the system. Audit staff understands that only two TOs, each of which has modest transmission assets, are not required to participate.

Finally, PJM shares a concurrent TOP registration with AEP, with AEP responsible for its facilities rated at 138 kV and below and PJM for facilities rated above 138 kV. However, audit staff determined that there are inadequate procedures or agreements in place between PJM and AEP governing reliability concerns that transcend the voltage levels of the BES, such as response to SOL or IROL exceedances. Audit staff

[44] The voltage schedule is a target voltage to be maintained within a tolerance band during a specified period.

[45] PJM Manual 03 at p. 32.

believes that PJM should ensure that it and AEP can effectively manage shared reliability risks that may require a coordinated TOP/TO response to avoid potential reliability gaps or overlaps.

In order to alleviate confusion regarding the entity responsible for specific tasks related to compliance with TOP Reliability Standards, and to provide clarity in the administration of CMEP activities, PJM should continue its process of clarifying which entity is responsible for the TOP Reliability Standards requirements for which PJM must comply.

Recommendations

We recommend that PJM:

25. Continue to review and update the TOP Matrix, PJM manuals, and other necessary documents to clarify responsibility for, and performance of, reliability tasks and eliminate any gaps or overlaps.

26. Coordinate its review in response to Recommendation 25 with NERC, the CEAs, and other parties to keep them informed of the process and provide them the opportunity to participate in the review.

27. Submit the results of its review in response to Recommendation 25 to the Division of Audits within 30 days after completion.

28. Coordinate with AEP to develop procedures for managing shared reliability risks that may require coordinated response to avoid potential reliability gaps or overlaps.

PJM Interconnection
Valley Forge Corporate Center
955 Jefferson Avenue
Norristown, PA 19403-2497

Robert V. Eckenrod
Senior Counsel
610.666.3184 | fax 610.666.8211
eckenr@pjm.com

September 27, 2012

VIA FEDERAL EXPRESS AND E-MAIL

Bryan K. Craig, Director and Chief Accountant
Division of Audits
Office of Enforcement
Federal Energy Regulatory Commission
888 First Street, NE, Room 5K-13
Washington, D.C. 20426

RE: FERC Audit No. PA11-21-000 – Revised Draft Audit Report

Dear Mr. Craig:

In response to the revised draft audit report issued on September 19, 2012, in the above-referenced matter, PJM Interconnection is pleased to provide you with one electronic copy and one original copy of the corresponding responses to the draft audit report.

If you have any questions, or if you require any further information, please contact me at your convenience.

Sincerely,

Robert V. Eckenrod
Senior Counsel

PJM Response to the Federal Energy Regulatory Commission (FERC) Audit of PJM Interconnection, L.L.C.'s Performance as a Table 1 Entity Responsible for Certain CIP Reliability Standards, and as a NERC-Registered Transmission Operator and Transmission Planner.

Docket No. PA11-21-000

September 27, 2012

Contents

Findings and Recommendations of the 2011 FERC Performance Audit of PJM

A. Performance Enhancements

1. Identifying Critical Assets and Associated Critical Cyber Assets

PJM's process for identifying CAs and associated CCAs needs to be enhanced to ensure that all CAs and associated CCAs related to the reliability or operability of the BES are properly identified. These enhancements will help PJM ensure no potential gaps exist in its process for identifying CAs and associated CCAs.

Recommendation #1

1. Revise its processes of identifying CCAs to incorporate all of the suggested guidance issued by NERC.

PJM Response:
Generally, PJM agrees with the recommendation to revise its process of identifying CCAs associated with PJM's CAs. As part of our annual review of the Risk Based Assessment Methodology (RBAM), PJM will review NERC's guidelines on Identifying Critical Assets with special attention to Table C3 and revise our Risk Based Assessment Methodology as necessary.

However, PJM would like to point out that PJM's CEA reviewed and audited PJM's application of its RBAM and concurred with PJM's assessment that the assets referenced by audit staff in the draft report were not performing functions critical to reliability and operability of the BES.

Additionally, while PJM will consider incorporating all of the elements of the applicable NERC guidance, PJM will continue to treat NERC guidance as instructive for consideration, but not compulsory. However, PJM will ensure that it documents its evaluation and set forth its justification in adopting or not adopting that guidance.

2. Access to Critical Cyber Assets

PJM needs to improve its processes and procedures for managing employees' logical (i.e. electronic) access rights to CCAs for access changes and for terminating access rights of employees to CCAs. PJM should improve its performance by eliminating its reliance on a decentralized, manual process for implementing change requests and removing employees' access rights to CCAs.

Recommendation #2

2. Expedite the development and implementation of an automated, centralized process for managing logical access rights to CCAs that includes controls to address the concerns identified in the audit.

PJM Response:
PJM agrees with the recommendation to expedite the development and implementation of an automated, centralized process for managing logical access rights to CCAs. This process began in early February 2012, and includes staff members that are dedicated to the data cleansing. In addition, PJM is now fully engaged with a proven service vendor to assist in this effort. In the interim, PJM's Business Compliance Services department has tasked a project team with identifying and implementing mitigating activities until this process can be fully automated.

Recommendation #3

3. Strengthen its policies and procedures going forward to include requirements that all account access changes be communicated to responsible parties so that these parties are aware what access changes have been made, and are required to verify that each change is appropriate.

PJM Response:
PJM agrees with the recommendation to strengthen its policies and procedures going forward to include requirements that all account changes be communicated to all responsible parties.

PJM's Business Compliance Services department has implemented processes to support our policies and procedures that enhance our internal communication and validation of information and authorization of accounts residing on PJM critical assets. Examples of these enhancements are quality assurance checks for provisioning accuracy, the creation and dissemination of ITS desktop procedures and full quarterly reconciliations of electronic access to PJM's Critical Cyber Assets.

Recommendation #4

4. Revise its policies and procedures to assign reasonable expiration dates to transferred employees' old logical access rights and to require periodic action to extend the access rights of such transferred employees. If access is needed beyond the initially assigned expiration date, PJM's policies should, at a minimum, permit an extension only by prompting required action on the part of the responsible party.

PJM Response:
PJM agrees to revise its policies and procedures to require explicit requests from management for personnel to retain access upon a transfer. This updated policy and procedure will note that if continuing access is not requested, access will expire within a reasonable amount of time.

3. Personnel Risk Assessments

PJM should continue to enhance its processes and procedures for documenting and tracking PRAs because PJM's method of tracking PRAs contained manual processes that led to three instances in which the wrong PRA dates were entered into PJM's tracking system. While these errors did not result in violations of the Reliability Standards, the manual processes created the potential for PJM to untimely update PRAs, which could lead to violations of CIP Standard requirements and potential risks to security.

Recommendation #5

5. Consider migrating to an automated system for processing PRAs. PJM should assess whether it is beneficial to automate the transfer of hire dates and PRA dates from its Human Resources system to its security training tracking system through the use of database technology.

PJM Response:
PJM agrees with the recommendation that the automation of PRA dates from the Human Resources system and the use of additional database technology will reduce potential errors as a result of less manual processes.

PJM is currently reviewing several internal processes in an effort to automate and ultimately eliminate additional data entry. As a result of the initial review, PJM has implemented a new system with automated workflows allowing users to enter data (i.e. PRA dates) into one database. Once entered, the data populates respective repositories for information concerning PRA dates as well as initial and annual security training dates.

Recommendation #6

6. Implement (if PJM decides not to employ automated procedures for PRAs) processes and procedures to validate data manually entered into (1) its Human Resources system related to hire dates and PRA dates, and (2) its security training spreadsheet.

PJM Response:
In addition to agreeing with the recommendation to implement automated processes for tracking PRAs, PJM also agrees with recommendation 6 and, as such, has implemented a number of changes regarding data validation and will continue to

make enhancements in this area. For example, PJM currently conducts a system synchronization process. An automated workflow has been created to compare hire dates, PRA dates as well as initial and annual security training dates to ensure accuracy of names and required dates for each individual. Additionally, PJM has designated a point person for PRA processing, training dates and system record(s).

4. Inventory of Software within the Electronic Security Perimeter

PJM's tracking of software on its CAs within its ESPs did not capture some of the supporting software packages that were installed as part of the main software package. Audit staff believes PJM needs to improve its ability to track software within its ESPs to ensure that all security patches and upgrades are timely implemented and documented.

Recommendation #7

7. Perform an inventory of software installed on each asset within its ESPs using all available tools and controls to develop a baseline inventory of software.

PJM Response:
PJM agrees with this recommendation to enhance its procedures and controls to maintain a complete and current inventory of all software installed on assets within the ESP.

PJM's updated procedures, which were implemented in the third quarter of 2011 prior to the deployment of a significant number of cyber assets, include the use of additional tools and layers of employee review. PJM will continue to leverage the enhancements created by these procedures to confirm that all software which resides on all other cyber assets within in its ESPs has been identified.

Recommendation #8

8. Strengthen its configuration management process, including enhanced procedures for conducting periodic reviews of assets within PJM's ESPs, to ensure PJM maintains an accurate inventory of installed software on all such assets.

PJM Response:
PJM agrees with the recommendation for strengthening its configuration management processes to ensure that it maintains an accurate inventory of installed software. PJM will investigate methods available to implement or modify existing controls to ensure that the software inventory is updated after the incorporation of applicable significant changes.

5. Electronic Security Perimeter Access Points

PJM's processes for conducting port scans of both its ESP access points and the CCAs within the ESPs should be enhanced to ensure PJM remains aware of all ports that may

be enabled. Such enhancements will increase PJM's performance in this area, allowing PJM more effectively to ensure only necessary ports and services are enabled and prevent unauthorized access to CCAs.

Recommendation #9

9. Consider enhancing its policies and procedures for conducting port scans on its access points to the ESPs to verify comprehensively that only necessary ports and services are open.

PJM Response:
PJM agrees with the recommendation to enhance its policies and procedures related to its existing port scan process for ESP access points. PJM plans to accomplish this by using a credentialed security audit approach.

6. Change Control and Configuration Management

PJM should enhance its processes and procedures governing its CCCM because PJM employees did not properly follow them in three instances during the audit period. While audit staff is encouraged that PJM was able to discover these instances, PJM should enhance its preventative measures to emphasize the importance of following the CCCM processes and procedures and preventing unauthorized changes to its systems.

Recommendation #10

10. Enhance its CCCM processes and procedures to include additional preventative measures to reinforce the importance of following its CCCM processes and procedures, such as providing additional training to relevant staff.

PJM Response:
PJM agrees with the recommendation to enhance its CCCM processes and procedures to include additional preventative measures to reinforce the importance of following its CCCM processes and procedures. PJM has already implemented a process which requires individuals who deviate from the established CCCM processes and procedures to complete additional training. In addition, PJM is actively working towards improving the CCCM training for individuals who have been authorized to make changes to cyber assets to emphasize that they must comply with the NERC CIP standards and each of PJM's controls.

7. Planning and Operating Models

PJM should enhance its policies and procedures governing its planning and operating models to minimize inaccuracies and inconsistencies by:

- Improving its procedures for developing and validating its planning models to ensure all significant changes made to elements of the PJM system are reflected in the models; and
- Developing documented procedures for validating and benchmarking the performance of its operating models to ensure consistency in the model data between PJM and its Transmission Owners (TOs).

Recommendation #11

11. Continue to enhance its policies and procedures in place, including the implementation of PJM's automated software, to verify its planning models are current and consistent before using these models in PJM's planning activities.

PJM Response:

PJM agrees with the recommendation to continue to enhance its policies and procedures related to verification of planning models before their use in PJM's planning activities. In fact, immediately following upon this event in 2010, and well before the initiation of the FERC performance audit, PJM made significant enhancements to its policies and procedures in this regard. As a near term solution, PJM continues to improve the existing technical desk references related to PJM planning. The updated library will include additional detail regarding the planning process and procedures as well as application of a common format and style.

PJM also recognizes the importance of a continued focus on data verification, and therefore has been testing and developing internal documentation for the planned future use of the Siemens Model on Demand software package. This tool is in various stages of development and production among several of PJM's neighboring entities. PJM sees this tool as an opportunity to improve model building and verification of planning models before use in planning and PJM expects that it will provide numerous benefits upon its implementation. However, for the purposes of this recommendation, it should be emphasized that the completion of this automated software is not imminent. As such, there is some consideration that an estimate for the completion of the recommendation requiring implementation of automated software could be imprecise and difficult to predict with great accuracy.

Nevertheless, PJM agrees that it will review all available opportunities to enhance its policies and procedures to verify its planning models are current and consistent, recognizing, however, that those process improvements may, or may not, include the implementation of the referenced automated software due to feasibility or availability concerns.

Recommendation #12

12. Develop criteria and requirements for communicating information about significant changes on the PJM system between the TOs and PJM to ensure that these changes are reflected timely in PJM's Planning Models.

PJM Response:
PJM agrees with the recommendation to develop criteria and requirements for communicating information about significant changes on the PJM system between the TOs and PJM to ensure that these changes are reflected timely in PJM's Planning Models. PJM's current procedural documentation (PJM Manual 14B: PJM Region Transmission Planning Process, Attachment H: Power System Modeling Data) focuses mainly on the annual update process and procedure. PJM will expand the scope of this procedure to include criteria and requirements for timely communication of significant changes on the PJM system between the TOs and PJM.

Recommendation #13

13. Develop a formal procedure to validate PJM's EMS Model and benchmark its performance to mutually agreed upon criteria in collaboration with TOs before deploying the EMS Model into use for real-time operations.

PJM Response:
PJM agrees with the recommendation to develop a formal procedure to validate PJM's EMS Model and benchmark its performance to mutually agreed upon criteria in collaboration with its Transmission Owners before deploying the EMS Model into use for real-time operations.

Key among the procedural changes that have already been implemented is a requirement by PJM's Transmission Owners to review PJM's pre- and post-construction configurations before any new equipment is commissioned for service. PJM also engages TO staff in the PJM Data Management Subcommittee which meets regularly to discuss modeling philosophy; to exchange information about planned model changes; and, to identify and/or review potential process improvements.

8. Plan to Continue Reliability Operations

On page 38 of the draft audit report, the following statement summarizes audits staff's recommendations in this area:

> PJM should update its contingency plan to include: (1) a list of the critical transmission facilities to be monitored; (2) procedures and responsibilities for conducting annual tests of the plan; (3) procedures and responsibilities for

providing annual training to implement the plan; (4) procedures for managing SOLs and IROLs; (5) procedures for performing congestion management and generation dispatch; and (6) procedures for continuing reliability operations in the event a TO without a fully functioning backup control center has its primary control center become inoperable.

PJM agrees with the Audit Team's assessment that PJM can enhance its plan to continue reliable operations by further consolidating many of the elements of its plan into a more centralized document. However, as a point of clarification, items four and five in the discussion only apply in the event both of PJM's 24/7 control centers are lost.

Recommendation #14

14. Update its contingency plan to include the list of critical transmission facilities and procedures for monitoring them.

PJM Response:
PJM agrees with the recommendation. As correctly recognized by audit staff in the draft report, during the course of audit fieldwork PJM made corrective actions to address audit staff's recommendation by updating its contingency plan to include the list of critical transmission facilities and procedures for monitoring them.

Recommendation #15

15. Update its contingency plan to include a full list of systems/applications to be covered by the plan.

PJM Response:
PJM agrees with the recommendation however, it also believes that a full list of systems/applications is covered by its contingency plan as contained in version 3 of Procedures for Communication/Application Failures. This document was specifically referenced in Operating Memo 45, and predates this audit. This was provided to the FERC on June 11th, 2012, in response to Data request # 109.

Recommendation #16

16. Update its contingency plan to include procedures and responsibilities for conducting annual tests of the plan and for providing annual training to implement the plan.

PJM Response:
PJM agrees with the intent of the recommendation. However, PJM had procedures and responsibilities for conducting annual tests of the plan and for providing annual

training to implement the plan PJM could benefit by further consolidating these plans. As correctly recognized by audit staff in the draft audit report, during the course of audit fieldwork PJM made corrective actions to address audit staff's recommendation by updating its contingency plan by consolidating a number of references.

Recommendation #17

17. Develop procedures in its contingency plan for (1) manually managing SOLs and IROLs, and (2) performing manual congestion management and generation dispatch in the event both its control center becomes inoperable.

PJM Response:
Generally, PJM agrees with the recommendation. Although PJM maintains that it does have significant redundancy in its dual 24/7 control centers, during the course of audit fieldwork PJM made corrective actions to address audit staff's recommendation by developing procedures in its contingency plan for (1) manually managing SOLs and IROLs, and (2) performing manual congestion management and generation dispatch in the event that both of its 24/7 control centers become inoperable. PJM believes that such capability will provide PJM tertiary capability to operate reliably.

Recommendation #18

18. Develop procedures in its contingency plan for continuing reliability operations in the event that a TO without a fully functioning backup control center has its primary control center become inoperable.

PJM Response:
PJM agrees with the recommendation to develop procedures in its contingency plan for continuing reliability operations in the event that a TO without a fully functioning backup control center has its primary control center become inoperable.

While the audit report states that there are three TOs in PJM's footprint that do not have a functional backup control center, it should be emphasized that there is only one PJM Transmission Owner without a fully functioning backup control center. To this point, this TO has an aggressive plan to install a functional backup control center, and their plans currently call for that facility to be in service by December, 2013.

In the interim, as part of its Emergency Operations Plan, this Transmission Owner has developed a comprehensive plan to supply PJM with data on their critical facilities in the event that its primary control center becomes inoperable.

B. Other Matters

1. System Operating Limits

The following summary is set forth on page 43 of the draft audit report[1]:

Audit staff understands that PJM monitors and has operational responsibility for the facilities in its footprint rated below 230 kV. PJM performs these responsibilities pursuant to thermal limits and associated facility ratings, even though PJM excludes such facilities in its definition of SOL in its operations horizon. Audit staff believes that PJM should strengthen its performance by defining SOLs consistently for the entire BES, and not just for facilities rated at 230 kV and above. Therefore, PJM should define SOLs for BES facilities rated at least from the 100 kV level. This practice would enhance PJM's ability to track and analyze SOL exceedances, and would increase transparency through PJM reports involving SOL exceedances, where applicable, to NERC and its Compliance Enforcement Authorities (ReliabilityFirst and SERC).

Generally, PJM agrees with audit staff's recommendation, but emphasizes that the authority and ability to direct the operation of facilities to prevent SOL exceedances has always existed and is not changed by the SOL definition change. PJM has operated to control for all BES equipment as well as sub-BES equipment since the BES definition was formalized.

Recommendation #19

19. Continue its review of its SOL methodology, and define SOLs for BES facilities rated at least from the 100 kV level and above.

PJM Response:
PJM agrees with this recommendation, and has already completed a review of its SOL methodology. PJM released Revision 8 of Manual 37 that revised the SOL definition to include all 100kV and select sub-100kV equipment. The revised definition reads:

> *"All BES facilities and "Reliability and Markets" sub-BES facilities as listed on the PJM Transmission Facilities page that are not considered IROL facilities are considered System Operating Limits (SOL)."*

This definition change does not impact how PJM controls facility loading, therefore there are no Operations or Markets impacts as a result.

[1] This discussion is also found on page 4 of the draft audit report.

Recommendation #20

20. Keep NERC, the CEAs, and other parties informed of PJM's review of its SOL methodology and provide them the opportunity to participate in the review of the findings.

PJM Response:
PJM agrees with the recommendation and has completed its review of its SOL methodology. PJM will send NERC and the CEAs the revised SOL methodology. However, it should be noted that because PJM has already taken action in this regard, NERC and the CEAs will not have the opportunity to participate in the review. As such, PJM would recommend that audit staff consider amending recommendation 20 to remove the requirement that PJM provide NERC and the CEAs the opportunity to participate in the review.

2. Interconnection Reliability Operating Limit

The following summary is set forth on page 47 of the draft Audit Report

Through discussions with PJM staff, audit staff found that PJM has defined two IROLs in its footprint that are based on 15-minute thermal ratings of equipment (i.e., 15- minute load dump rating) that, if operated at or potentially above those ratings, will afford system operators a maximum of only 15 minutes to return the system below the IROL limit. Audit staff expressed concern that PJM's procedures, as discussed above, which afford the operators 30 minutes to mitigate an IROL exceedance, may not be adequate to address these IROLs.

The 15-minute rating and potential relay action concern is only applicable for an actual overload on the equipment. PJM operates on a pre-contingency basis such that PJM is constantly monitoring and taking actions to ensure that *simulated* post-contingency flows are within SOL limit, which would be the Emergency Rating. For these two facilities, PJM has gone a step further to indicate that if the 15-minute Load Dump rating is exceeded on a *simulated* post-contingency basis PJM allows its operators a maximum of 30-minutes to implement corrective actions to control the *simulated* post-contingency flow below the Load Dump rating. (NOTE: No equipment is exceeding its actual rating. Actual flows are below normal limits, and to clarify what is being described is *simulated* post contingency flows in this scenario. Therefore, no equipment is exceeding a relay setting and there is no increased likelihood of tripping). If flows cannot be controlled, PJM will direct pre-contingency load shedding to restore the *simulated* post-contingency flows within the IROL limits. The reason PJM does this is to address the exact concern of this Audit Team and to prevent what occurred in the Southwest Blackout. That is, PJM is concerned that if post contingency flows exceed the last known rating, that facility

may relay out of service. PJM needs to give the operators some time to take those actions in the *simulated* post contingency scenario. To that affect, PJM allows 30-minutes for corrective action. However, it is very important to understand that if the actual flow were to exceed the 15-minute Load Dump rating, PJM will direct Load Shed immediately and the Transmission Owners are required to respond within 5-minutes. This further addresses the Audit Team's concerns regarding time to respond to the 15-minute rating.

PJM staff explained that these IROLs are rarely active, but that in the event of an actual exceedance of either IROL, PJM would take action with respect to this equipment within the 15-minute period to reflect the actual rating constraint. Audit staff notes that neither IROLs were exceeded during the audit period. However, audit staff believes that PJM should enhance its existing written procedures to ensure that it could respond within the 30-minute window to exceedances of these two thermal IROLs. Also, PJM needs to ensure that TO operators are aware of these IROLs.

The PJM IROLs are documented in three Manuals M-03, M-13 and M-37. Furthermore, M-13 included the Load Shed tables for the Transmission Owners. This Manual and table is reviewed at least annually through the stakeholder process which includes representatives from all Transmission Owners. Furthermore, the Audit Team acknowledged that PJM performs drills of the IROL Load Shed plan, which shows all Transmission Owners are responding.

Recommendation #21

21. Develop procedures for documenting formal lessons-learned resulting from load-shedding drills that are communicated to all parties involved.

Recommendation #22

22. Review load-shedding drill results and update governing policies and procedures to reflect the performance demonstrated in these drills.

PJM Response for Recommendation #21 and #22:
PJM agrees with the recommendations, and will review and update the policies and procedures referenced to enhance the load-shedding drill documentation requirements to ensure lessons-learned are communicated and to reflect performance demonstrated in the drills.

Recommendation #23

23. Enhance its policies and procedures to address scenarios involving IROLs with 15-minute load dump ratings.

PJM Response:
PJM agrees with this recommendation and will review its policies and procedures that address operational treatment of IROLs, and include as necessary, any enhancements to those policies and procedures.

Recommendation #24

24. Enhance its policies governing protective relay settings and associated IROLs to include procedures for operating above load dump ratings for the time required to take responsive action.

PJM Response:
PJM agrees with the recommendation, and continues to enhance its policies governing protective relay settings and associated IROLs for operating above load dump ratings.

PJM's current operating procedures ensure that protective relay settings are set such that they permit time for operators to take necessary actions to maintain reliability. However, PJM will look for opportunities where it can include procedures to assist the operators when they must operate above load dump ratings for the time required to take responsive action.

3. Compliance Enforcement for the Transmission Operator Function

PJM, with one exception, is registered as the sole TOP for the BES transmission facilities within its footprint. PJM carries out its TOP functions through assignment of particular TOP tasks to its member TOs. Audit staff believes that PJM should continue to strengthen the clarity of the identity of the entity responsible for performing specific TOP tasks in order to: (1) ensure there are no gaps or unnecessary overlaps in the performance of TOP tasks; (2) ensure all entities are aware of their assigned duties with respect to compliance with the Reliability Standards; and (3) better enable Reliability*First* and SERC, the CEAs for TOPs and TOs in PJM's footprint, to administer the NERC CMEP as it relates to PJM and its member TOs.

PJM Response:

Overall, as noted below, PJM agrees with the general recommendations of audit staff in this area. However, as a small point of clarification to the discussion set forth above, PJM is registered as the sole TOP for those BES transmission facilities that its Member Transmission Owners have transferred functional control to PJM in accordance with the provisions of PJM's Consolidated Transmission Owner's Agreement; not necessarily all BES transmission facilities within its footprint.

Recommendation #25

25. Continue to review and update the TOP Matrix, PJM manuals, and other necessary documents to clarify responsibility for, and performance of, reliability tasks and eliminate any gaps or unnecessary overlaps.
26.

PJM Response:

PJM does not believe that any reliability gaps exist in the performance of the TOP function; however, PJM agrees that continued coordination and review of the TOP matrix is a necessity to ensure responsibility and performance of reliability tasks are understood by all parties. In addition, PJM understands the FERC staff observation about ensuring there are no unnecessary task overlaps and, while some task overlaps may exist, PJM does not believe any authority overlaps in tasks exist that may obstruct reliability. PJM is ultimately responsible for the Reliability Coordinator function and as described in the Functional Model version 5: "The Reliability Coordinator may direct a Transmission Operator within its Reliability Coordinator Area to take whatever action is necessary to ensure that Interconnection Reliability Operating Limits are not exceeded." This ultimate authority of the Reliability Coordinator (PJM) will ensure that overlaps of reliability tasks only enhance reliability.

Maintaining a current TOP Matrix is a continuing process facilitated by PJM staff. Coordination between the PJM Manuals and NERC Reliability Standards takes place as each of the NERC Standards is revised or new standards are created. The TOP Matrix then recognizes the Manual changes and aligns the PJM Manual sections with the NERC requirements. As such, PJM believes its current processes are in alignment with the recommendation.

However, as noted above, PJM is concerned that this recommendation, as stated, does not established a finite objective, other than to continually review and update the TOP matrix.

Recommendation #26

27. Coordinate its review in Recommendation 25 with NERC, the CEAs, and other parties to keep them informed of the process and provide them the opportunity to participate in the review.

PJM Response:

In developing future versions of the TO/TOP matrix, PJM works with impacted parties to ensure coordination is taking place. PJM includes CEAs in the review process to provide them the opportunity to participate and PJM will continue this practice as recommended by FERC in the draft report.

As part of PJM's on-going review process, NERC and CEA staffs will be sent draft copies of the TOP Matrix before going through the full PJM approval process to allow comments and suggestions to be incorporated, if appropriate.

Recommendation #27

28. Submit the results of its review in Recommendation 25 to the Division of Audits within 30 days after completion.

PJM Response:
PJM will comply with all of the requirements under Section D. Compliance and Implementation of Recommendations (p. 8).

Recommendation #28

29. Coordinate with AEP to develop procedures for managing shared reliability risks that may require coordinated response to avoid potential reliability gaps or overlaps.

PJM Response:
PJM and AEP met on September 5, 2012 to discuss the status of their shared reliability risks. PJM and AEP will continue this coordination to address the FERC audit recommendation.

Document Content(s)