FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

In Reply Refer To:
Office of Enforcement
Docket No. PA12-11-000
July 18, 2013

Sara McCoy, Manager of Electric Reliability Compliance
Salt River Project Agricultural Improvement and Power District
P.O. Box 52025
Phoenix, AZ 85072

Dear Ms. McCoy:

1. The Division of Audits (DA) within the Office of Enforcement (OE), with the assistance of staff from the Office of Electric Reliability (OER), of the Federal Energy Regulatory Commission (Commission) has completed the audit of Salt River Project Agricultural Improvement and Power District (SRP) for the period from June 18, 2007, to March 26, 2013. The enclosed audit report explains our audit conclusions and recommendations.

2. The audit evaluated SRP's compliance with the requirements of the North American Electric Reliability Corporation's mandatory Reliability Standards, focusing on Bulk-Electric System Operations and Planning, and Critical Infrastructure Protection.

3. In its June 27, 2013 response, SRP said it agrees with all audit recommendations. A copy of SRP's verbatim response is included as an appendix to this report. I hereby approve the audit report.

4. Within 30 days of this letter order, SRP should submit a plan to comply with the recommendations. SRP should make quarterly submissions describing how and when it plans to comply with the recommendations, including the completion dates for each. The submissions 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 recommendations are completed.

5. 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. SRP 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).

6. 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.

7. I appreciate the courtesies extended to our auditors. 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

Reliability Audit of Salt River Project Agricultural Improvement and Power District

Docket No. PA12-11-000
July 18, 2013

Office of Enforcement
Division of Audits

TABLE OF CONTENTS

I. Executive Summary 1

A. Overview 1
B. Salt River Project Agricultural Improvement and Power District 1
C. Conclusions 2
D Recommendations 4
E. Implementation of Recommendations 5

II. Introduction 6

A. Objectives 6
B. Scope & Methodology 6
1. Critical Infrastructure Protection Standards. 8
2. Operations and Planning Standards. 10

III. Conclusions and Recommendations 12

A. Critical Infrastructure Protection Standards 12
1. Ports and Services for Critical Cyber Assets inside the Electronic Security Perimeter 12
2. Manual Log Review of Electronic Access 14
3. CIP-Related Training Sufficiency 16
4. Testing of Backup Media 19
B. Operations and Planning Standards 21
5. Plans for Loss of Control Center Functionality 21
6. Training for System Operators 24
7. Training for Distribution Operators on Load Shedding 26

I. Executive Summary

A. Overview

The Division of Audits within the Office of Enforcement, in conjunction with the Division of Compliance and Division of Reliability Standards and Security of the Office of Electric Reliability, has completed an audit of Salt River Project Agricultural Improvement and Power District (SRP). The audit was commenced to evaluate SRP's compliance with the requirements of the North American Electric Reliability Corporation's (NERC) mandatory Reliability Standards, focusing on Critical Infrastructure Protection (CIP) Standards and Operations and Planning (O&P) Standards. The timeframe for the audit included the entire period from June 18, 2007, to March 14, 2013, but focused on the last two years.

B. Salt River Project Agricultural Improvement and Power District

SRP, a political subdivision of the state of Arizona, provides retail electric service in a 2,900-square-mile territory that includes part of the Phoenix metropolitan area. It serves nearly one million customers at retail, and has over 4,000 employees.

SRP is registered in the Western Electricity Coordinating Council (WECC) region for 12 reliability functions, as defined in the NERC Compliance Registry: Balancing Authority (BA); Distribution Provider (DP); Generation Owner (GO); Generation Operator (GOP); Load-Serving Entity (LSE); Planning Authority (PA); Purchasing-Selling Entity (PSE); Resource Planner (RP); Transmission Owner (TO); Transmission Planner (TP); Transmission Operator (TOP); and Transmission Service Provider (TSP). This audit focused on SRP's responsibilities as a BA, TO, and TOP.

C. Conclusions

Audit staff found seven areas in which SRP could enhance its CIP and O&P compliance:[1]

- *Ports and Services for Critical Cyber Assets (CCAs) inside the Electronic Security Perimeter (ESP):* SRP implemented an active (i.e., live) scanning process to ensure that only ports required for normal and emergency operations of a CCA were open. However, it did not actively scan two types of its CCAs due to the technical characteristics of those two CCAs and the attendant risks inherent in performing such scans. To manage these risks, SRP relied primarily upon manufacturer documentation rather than scanning. This approach was less reliable than scanning in a test environment.

- *Manual Log Review of Electronic Access:* SRP relied on its automated log consolidator to monitor electronic access to its ESPs and performed manual log reviews only on a limited and ad hoc basis. As cyber attacks are constantly evolving, SRP should consider a defense strategy that includes some level of regular, manual log review coupled with SRP's other proactive techniques.

- *CIP-Related Training Sufficiency:* SRP's cyber security training, which was bifurcated between its NERC Cyber Security Training Program and its corporate cyber security training, did not adequately address all of the required areas. While SRP's NERC Cyber Security Training Program covered the necessary topics required by Reliability Standard CIP-004-3 R2, some aspects of the training were limited. For example, audit staff found a lack of details and examples on networking hardware and software, and electronic interconnectivity supporting the operation and control of CCAs. Only some of those details were included in SRP's separate corporate cyber security training. Further, certain SRP contractors did not receive comprehensive cyber security training since they participated only in the NERC Cyber Security Training Program, but did not receive SRP's corporate cyber security training.

- *Testing of Backup Media:* SRP used a sampling procedure when testing within its control center ESP for two categories of CCAs: CCAs that store backup data on the backup media, as well as the backup media itself. This procedure did not ensure that the information essential to recovery that was stored on backup media would be tested at least annually. One concern is that since the control center ESP had multiple categories of devices, the sampling used in the testing may permit several years to elapse before the information for all types

[1] A detailed discussion of these enhancements and associated recommendations is included in section III of this audit report.

of devices is tested to ensure that the essential information is available for recovery. A second concern is that while the server on which the backups reside is tested at least annually, it is possible that certain backup files may be corrupted. This situation may not be detected under SRP's procedure.

- *Plans for Loss of Control Center Functionality:* SRP did not fully test the viability of its contingency plan, which included procedures for dispatching qualified personnel to its twelve key substations to keep system operators informed of all alarms, analogs, flows, breaker operations, and operational limit violations at each substation. SRP's testing of its contingency plan was not robust, as it was based on dispatching personnel to only two of its twelve key substations.

- *Training for System Operators:* SRP modified its training for its system operators on the characteristics of its generation resources as a result of the lessons learned during the February 2011 cold weather event. Audit staff commends SRP on its independent review, but is concerned that: (1) SRP did not conduct this training on a recurring basis; and (2) SRP did not document the attendance at and completion of initial training provided to newly hired operating personnel.

- *Training for Distribution Operators on Load Shedding:* SRP's training on load-shedding procedures for its distribution operators was more frequent as a result of lessons it learned during the February 2011 cold weather event. However, audit staff found that the training could be made more effective by including simulations and drills.

D. Recommendations

Audit staff suggests SRP adopt the following recommendations to implement the enhancements described in this audit report:

1. Consider implementing process enhancements for scanning ports and services to further minimize risk to its ESPs. For example, such enhancements may include the scanning of an identically configured relay in a lab environment to determine with certainty what ports and services may be open on the CCA.

2. Develop formal processes and procedures for manual log review to detect actual or attempted unauthorized access to its ESPs. Procedures for conducting the manual log reviews should specify a regular interval between such reviews.

3. Strengthen its cyber security training program(s) by reviewing all training materials to ensure that its cyber security training adequately covers networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of CCAs. This review may include a gap analysis to determine if any necessary details are missing from its NERC Cyber Security Training Program or corporate cyber security training.

4. Strengthen its cyber security training program(s) by including examples that provide additional context to the training.

5. Provide SRP's contractors and service providers with the same cyber security training that is provided to SRP employees whose activities are subject to compliance with CIP-004-3.

6. Consider revising its backup media testing procedures to ensure that the control center storage media themselves are more rigorously tested, and that at least one CCA from each category of assets within the control center ESP should be tested on an annual basis.

7. Implement its planned upgrades to RTU communications to the EDC as soon as possible.

8. If implementation of its planned upgrades to RTU communications to the EDC will take longer than six months from the date of this audit report, SRP should in the meantime develop a means to test its existing contingency plan for dispatching personnel to key substations, and conduct such a test.

9. Conduct a review of its training program for its operating personnel, and implement remedies to strengthen the program, including remedies that measure the effectiveness of the training provided.

10. Include training on the operating characteristics of SRP's generators as part of the recurring training for operators.

11. Develop procedures for more detailed documentation of the attendance at and completion of initial training (both classroom and on-the-job) for newly hired operating personnel.

12. Develop and implement training for its distribution operators that includes, at least annually, simulations and drills on load shedding and restoration. The goal of such training should be to ensure that SRP's distribution operators are capable of using the load-shedding (rotating blackout) capability of their Energy Management System (EMS)/Supervisory Control and Data Acquisition (SCADA) systems.

E. Implementation of Recommendations

Audit staff further recommends that SRP:

- Submit for audit staff's review its plans for implementing this report's recommendations. SRP 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 SRP's progress in completing each action recommended in the final audit report. SRP 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 SRP completes all recommended corrective actions.

- 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 SRP's completion of any such document.

II. Introduction

A. Objectives

Our objectives were to evaluate SRP's compliance with the requirements of NERC's mandatory Reliability Standards and to make recommendations to SRP for specific enhancements. The O&P Reliability Standards, which the Commission initially approved in its Order No. 693, were designed to support reliable operation of the Bulk-Power System.[2] The CIP Reliability Standards, which the Commission initially approved in Order No. 706,[3] provide a framework for identifying and protecting CCAs to support the reliable operation of the Bulk-Power System.[4]

B. Scope & Methodology

This audit was undertaken to test SRP's compliance with mandatory Reliability Standards and to point to areas where the effectiveness and efficiency of SRP's operations and cyber security practices could be improved. Audit staff planned the audit using a risk-based approach that identified topics for testing based on a review of frequently violated Reliability Standards, previous audits conducted by WECC, SRP self-reported and WECC-alleged violations, Notice of Penalty filings, and Bulk-Electric System (BES) events involving SRP. The audit focused on SRP's compliance with the Reliability Standards, the company's implementation of activities relating to those standards, and areas where SRP could enhance reliability and security in the audited areas.

Audit staff also evaluated SRP's response to NERC alerts that were applicable to SRP's registered functions. Specifically, audit staff verified that designated SRP personnel monitored such NERC alerts and notified departments that may have been

---

[2] *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).

[3] *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).

[4] Audit staff audited to the CIP v3 Reliability Standards. The Commission approved CIP v3 after Order No. 706; the requirements we audited were essentially unchanged from the CIP v1 counterparts approved in Order No. 706.

impacted by the NERC alerts. Further, audit staff examined SRP's actions in response to each applicable NERC alert. Audit staff notes that its review in this area did not uncover any concerns related to SRP's responses to NERC alerts.

SRP cooperated fully with all of audit staff's requests for information, access to facilities, and access to SRP employees. Throughout the audit, SRP readily made its subject-matter experts available to address audit staff's questions and concerns. These subject-matter experts were open and transparent in their discussions with audit staff, which greatly assisted our testing and evaluations.

Audit staff performed the following steps to facilitate the testing and evaluation of the audit objectives:

- *Reviewed Public Information* – Audit staff reviewed publicly available materials on the FERC and SRP web sites and other key industry and news sources.

- *Identified Standards and Criteria* – Audit staff identified standards and criteria to use in evaluating the company's compliance with NERC rules, regulations, and other requirements. Sources included the NERC Reliability Standards, Commission orders and regulations, and internal company policies and procedures relevant to audit objectives.

- *Obtained Input From Regional Entity Staff* – Audit staff conferred with WECC staff during the audit. WECC staff provided valuable information and insight given WECC's role as the Compliance Enforcement Authority in the Western Interconnection. Discussions with WECC staff included SRP's reliability history, risk areas, and other areas of concern.

- *Conducted Site Visits* – Audit staff conducted two site visits to SRP offices and operational facilities in the Phoenix, AZ, metropolitan area. During these site visits, audit staff: (1) reviewed and tested SRP's internal policies and procedures relevant to audit objectives; (2) reviewed SRP's regulatory and corporate compliance programs; (3) toured SRP's primary control room, backup control center, and areas where distribution control, generation dispatch, and wholesale power purchases were performed; (4) discussed SRP's training program, verified training received by employees, and reviewed SRP's processes to record and monitor such training; and (5) evaluated and determined the relevance (for purposes of this audit) of processes for responding to NERC alerts.

- *Interviewed SRP Employees* – Audit staff conducted numerous interviews and teleconferences with SRP's compliance staff, subject-matter experts, and

senior management to support the audit team's evaluation of compliance with Commission rules, regulations, and other requirements.

- *Issued Data Requests* – Audit staff issued numerous data requests to gather information during this audit. Information requested included: organizational charts; internal policies, processes, procedures, and controls; SRP's internal audits and reviews; documentation of the company's compliance activities; performance metrics developed internally by SRP; operational data; documentation related to the company's governance, compliance budget, and compliance culture; corrective actions implemented as a result of system events; actions taken in response to NERC alerts; and other key information.

- *Provided improvement recommendations* – Audit staff orally presented to SRP several recommendations to improve in areas within the audit scope. These recommendations were informally given during the site visit and touched on areas relating to consistency among document retention policies; improving access to operating procedures for distribution operators; strengthening its compliance documentation by addressing minor discrepancies found in internal procedures; ensuring consistency in version history numbering, standardizing nomenclature accordingly, and adding additional detail; and improving processes and procedures for intra-company coordination between SRP employees in different business functions to identify, track, and report disturbance events.

Audit staff also examined the effectiveness of SRP's policies, processes, procedures, manuals, training program and materials, and other criteria that SRP employed to achieve compliance. For example, audit staff conducted testing in the following areas:

1. Critical Infrastructure Protection Standards

- *Assessment and identification of Critical Assets(CAs) and associated Critical Cyber Assets (CCAs)*

To evaluate SRP's assessment to identify CAs and associated CCAs, audit staff with CIP and O&P expertise reviewed data responses and interviewed SRP personnel on each step of the company's Risk-Based Assessment Methodology, including the personnel involved and the analysis performed to identify each critical asset.

- *Electronic security perimeter (ESP) and physical security perimeter (PSP) designation and protection.*

  To verify that SRP had designated and implemented required controls for its ESPs and PSPs, audit staff interviewed SRP personnel and analyzed company policies and procedures for designating ESPs, implementing security controls, and defining and protecting its PSPs. Also, audit staff evaluated SRP's remote-access policies and controls for access to SRP's ESPs.

- *Personnel risk assessment, and access control policies, procedures, and controls related to CCAs.*

  To evaluate the effectiveness of SRP's personnel risk assessment process, audit staff issued data requests and held interviews with SRP staff to discuss SRP's policies, procedures, and controls for personnel risk assessments, including the scope of the assessments, the agreement between SRP and the vendor that performed risk assessments for SRP, coordination with Federal agencies for assessments of foreign nationals, and controls in place to ensure cyber access was removed when a personnel risk assessment expired. Audit staff also tested SRP's controls for maintaining a list of personnel who had authorized unescorted physical access to CCAs and tested to determine if any employees who changed positions or employment status had their access updated as necessary.

- *System security management policies, procedures, and controls related to CCAs*

  To evaluate the effectiveness of SRP's system security management procedures, audit staff interviewed SRP personnel and examined the company's policies and procedures related to change and configuration management, vulnerability assessment, testing, and ports and services to determine if SRP had specific, defined policies and procedures for each subject area covered by the procedures.

- *CCA recovery plans*

  To verify that SRP had documented recovery plans for its CCAs as required, audit staff reviewed the company's policies and procedures describing how it exercised and updated its recovery plans for each class of CCAs, as needed. Audit staff also interviewed SRP personnel to clarify its understanding of the recovery plans.

2. Operations and Planning Standards

- *Resource and demand balancing*

  To test how SRP complied with Reliability Standard BAL-004, audit staff evaluated the company's internal controls in place to ensure SRP's compliance with requirements to: (1) notify other BAs when it operated in an Automatic Generation Control operating mode other than Automatic Time Error Correction (ATEC); and (2) ensure that it did not have ATEC out of service for more than 25 hours per calendar quarter when synchronously connected to the Western Interconnection.

- *Communications and coordination protocols*

  To verify that SRP had communications procedures and protocols as required by Communications (COM) Standards, audit staff reviewed documentation providing an overview of SRP's control center communications, as well as communications agreements between SRP and its neighboring entities. Audit staff reviewed SRP's internal controls to ensure its generation and transmission operators used three-part communication as required when directives were issued. In addition, audit staff issued data requests and interviewed SRP system operators on communications protocols used during emergency conditions, as required by Emergency Preparedness and Operations (EOP) Standards.

- *Planning and implementation of emergency operations*

  To verify that SRP had procedures in place as required by EOP Standards for automatic and manual load shedding, including SRP's curtailment plan, pre-load shedding checklist, and control center recovery plan, audit staff issued data requests and interviewed SRP system and distribution operators. Audit staff toured the backup control center facilities to verify SRP's ability to implement its recovery plan. Similarly, audit staff issued data requests and interviewed SRP operational staff regarding its blackstart plan.

- *Staff qualifications and training*

  To examine whether SRP had implemented procedures for training personnel in accordance with the Personnel Performance, Training, and Qualifications (PER) Standards, audit staff issued data requests and held interviews with SRP managers and operating personnel. Those data requests and interviews addressed the company's training program for system and distribution operators; specific topic areas covered by the operator training and the periodicity of training; training materials; processes to monitor employees' training requirements and maintenance

of records of completed training; and load-shedding procedures for system and distribution operators.

- *Blackstart testing plans*

  To verify that SRP had procedures to verify the feasibility of its blackstart plan as the EOP Standards required, audit staff interviewed SRP operational staff regarding the company's blackstart plan and also reviewed SRP's restoration plan and blackstart resource-testing requirements.

III. Conclusions and Recommendations

A. Critical Infrastructure and Protection Standards

1. Ports and Services for Critical Cyber Assets inside an Electronic Security Perimeter

SRP implemented an active (i.e., live) scanning process to ensure that only ports required for normal and emergency operations of a CCA were open. However, it did not actively scan two types of its CCAs due to the technical characteristics of those two CCAs and the attendant risks inherent in performing such scans. To manage these risks, SRP relied primarily upon manufacturer documentation rather than scanning. This approach was less reliable than scanning in a test environment.

Pertinent Guidance

CIP-007-3 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.

> **R2.1.** The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
>
> **R2.2.** The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> **R2.3.** In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

Background

Audit staff reviewed documentation provided by SRP about its ports and services and found that SRP's process for determining open ports/services varied depending upon each system/environment and could include: (1) actively scanning via Network Management Application Program (NMAP), Nessus, nCircle, or other scanner; (2) examining a configuration file or security policy; or (3) relying on the vendor.

The ports and services related to SRP's scanning process were logical connections designed to uniquely identify different applications or processes running on a single computer, which thereby enabled those applications or processes to share a single physical connection to a network. By performing a scan, SRP could determine if a port unexpectedly was open and therefore capable of receiving and transferring data. Accordingly, an unexpectedly open port is a sign that an unnecessary service, which can have its own set of vulnerabilities, was not disabled properly. Running unnecessary services increases the potential risk of an unauthorized intruder gaining or attempting to gain access to the cyber asset through those vulnerabilities. Therefore, the potential risk of an unauthorized user gaining access to the CA can be minimized by identifying the number and status of ports, and ensuring that only ports necessary for normal and emergency operations are open.

During field testing, audit staff confirmed that SRP did not conduct scans on all of its CCAs. Specifically, two types of highly sensitive relays were excluded from scanning. Audit staff concurs that excluding these devices from active scanning is appropriate. To manage the risk of not actively scanning these relays, SRP explained that it referenced manufacturer documentation regarding them to determine the ports necessary to be open and the settings of these and all other ports to these assets. Audit staff notes that it found no evidence that SRP's scanning activities, including the absence of scanning of these two types of devices, had resulted in any unauthorized access.

Audit staff recognizes the critical function of these relays, and agrees with SRP that these relays may demonstrate an adverse reaction if scanned. However, audit staff's view is that relying on vendor documentation as the sole means to ensure that only those ports and services for normal and emergency operations are enabled increases risk that undocumented ports and services will be open. Audit staff understands that SRP has a lab environment where it could scan an identically configured relay to determine with certainty what ports and services are open on the CCA. Such scanning would enhance SRP's current practice and could minimize risk to its ESPs through increased awareness of what ports and services are open on the relays.

Recommendations

Audit staff recommends that SRP:

1. Consider implementing process enhancements for scanning ports and services to further minimize risk to its ESPs. For example, such enhancements may include the scanning of an identically configured relay in a lab environment to determine with certainty what ports and services are open on the CCA.

2. Manual Log Review of Electronic Access

SRP relied on its automated log consolidator to monitor electronic access to its ESPs and performed manual log reviews only on a limited and ad hoc basis. As cyber attacks are constantly evolving, SRP should consider a defense strategy that includes some level of regular, manual log review coupled with SRP's other proactive techniques.

Pertinent Guidance

CIP-005-3 R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

In FERC Order No. 706, the Commission articulated the benefits of supplementing automated log review with manual log review on a regular basis with respect to detecting unauthorized attempts to access, and accesses to ESPs. For example, paragraph 526 states:

> Requirement R3 of CIP-005-1 does not currently require a responsible entity to manually review logs if it has alerts. However, the Commission continues to believe that, while automated review systems provide a reasonable day-to-day check of the system and a convenient screening for obvious system breaches, periodic manual review provides the opportunity to recognize an unanticipated form of malicious activity and improve automated detection settings. Further, manual review is beneficial to judge the effectiveness of protection measures, such as firewall settings.[5]

Background

As a part of its processes to monitor electronic access to its ESPs, SRP had implemented an automated log consolidation tool capable of detecting unauthorized access or attempts to gain unauthorized access to its ESPs. This tool was also capable of sending email alerts to SRP personnel based on predefined monitoring criteria. In addition, SRP performed manual log reviews on an ad hoc basis. However, SRP did not have procedures for performing manual log reviews. As such, SRP relied primarily on its automated log consolidation tool. Audit staff believes that SRP can benefit from

[5] Order No. 706 at P 526.

modifying its electronic access monitoring processes and procedures to include regular, manual log reviews to supplement its automated tool.

Recommendations

Audit staff recommends that SRP:

2. Develop formal processes and procedures for manual log review to detect actual or attempted unauthorized access to its ESPs. Procedures for conducting the manual log reviews should specify a regular interval between such reviews.

3. CIP-Related Training Sufficiency

SRP's cyber security training, which was bifurcated between its NERC Cyber Security Training Program and its corporate cyber security training, did not adequately address all of the required areas. While SRP's NERC Cyber Security Training Program covered the necessary topics required by Reliability Standard CIP-004-3 R2, some aspects of the training were limited. For example, audit staff found a lack of details and examples on networking hardware and software, and electronic interconnectivity supporting the operation and control of CCAs. Only some of those details were included in SRP's separate corporate cyber security training. Further, certain SRP contractors did not receive comprehensive cyber security training since they participated only in the NERC Cyber Security Training Program, but did not receive SRP's corporate cyber security training.

Pertinent Guidance

CIP-004-3 R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

> **R2.1.** This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.
>
> **R2.2.** Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> > **R2.2.1.** The proper use of Critical Cyber Assets;
> > **R2.2.2.** Physical and electronic access controls to Critical Cyber Assets;
> > **R2.2.3.** The proper handling of Critical Cyber Asset information; and,
> > **R2.2.4.** Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

CIP-004-3 R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

In Order No. 706, the Commission said that: "[C]yber security training programs are intended to encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."[6]

Background

Audit staff reviewed documentation of SRP's cyber security training, which was bifurcated between a NERC Cyber Security Training Program and corporate cyber security training. Audit staff found that while SRP's NERC Cyber Security Training Program covered the necessary topics required by CIP-004-3, portions of the training could be clarified by including examples and greater detail. For example, the NERC Cyber Security Training Program referenced other related documents, but did not emphasize the salient points of those documents or provide examples to illustrate how the training applied to an employee's position. Audit staff believes that, by including these details in its NERC Cyber Security Training Program, SRP would strengthen the program by making it more accessible to the employees required to receive the training.

Audit staff found that SRP's NERC Cyber Security Training Program could be enhanced to further "encompass training on the networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of critical cyber assets."[7] For example, SRP provided presentation slides from its NERC Cyber Security Training Program as evidence of its cyber security training. The slides referenced a page on SRP's intranet where employees could find documents on several topics, including a procedure on sabotage reporting. However, the training slides did not identify the name of the procedure or address how to detect occurrences of physical or cyber sabotage. SRP could strengthen its cyber security training by including more details and highlighting the salient points from relevant documents instead of just mentioning that such documents exist. Also, the training identified numerous rules, but did not give examples related to those rules. Audit staff believes SRP can make its cyber security training more relatable to employees by including examples that give context.

SRP confirmed that some of the details mentioned above were covered in its separate corporate cyber security training, which all SRP employees were required to take. While the existence of the corporate cyber security training alleviated, in part, audit staff's concern about the lack of detail in SRP's NERC Cyber Security Training Program, audit staff believes that SRP could benefit from performing a gap analysis comparing its two cyber security training programs and revising its training program(s) to ensure that its employees and contractors both receive the appropriate training.

[6] Order No. 706 at P 434.
[7] *Id.*

Additionally, certain SRP contractors did not receive the complete cyber security training offered by SRP since they participated only in the NERC Cyber Security Training Program, but did not receive SRP's corporate cyber security training. Because these contractors did not receive all cyber security training available to SRP employees, audit staff recommends that the same training be provided to SRP's contractors as is provided to SRP employees whose activities are subject to compliance with CIP-004-3.

Recommendations

Audit staff recommends that SRP:

3. Strengthen its cyber security training program(s) by reviewing all training materials to ensure that its cyber security training adequately covers networking hardware and software and other issues of electronic interconnectivity supporting the operation and control of CCAs. This review may include a gap analysis to determine if any necessary details are missing from its NERC Cyber Security Training Program or corporate cyber security training.

4. Strengthen its cyber security training program(s) by including examples that provide additional context to the training.

5. Provide SRP's contractors and service providers with the same cyber security training that is provided to SRP employees whose activities are subject to compliance with CIP-004-3.

4. Testing of Backup Media

SRP used a sampling procedure when testing within its control center ESP for two categories of CCAs: CCAs that store backup data on the backup media, as well as the backup media itself. This procedure did not ensure that the information essential to recovery that was stored on backup media would be tested at least annually. One concern is that since the control center ESP had multiple categories of devices, the sampling used in the testing may permit several years to elapse before the information for all types of devices is tested to ensure that the essential information is available for recovery. A second concern is that while the server on which the backups reside is tested at least annually, it is possible that certain backup files may be corrupted. This situation may not be detected under SRP's procedure.

Pertinent Guidance

CIP-009-3 R5. Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site.

Background

Audit staff reviewed SRP's backup media testing procedures and interviewed SRP personnel about the implementation of these procedures. Audit staff found that all testing, other than for the control center ESP (which is a highly critical element for reliability), was conducted by SRP in a manner that was unambiguously consistent with the requirements of CIP-009-3.

However, for its control center ESP, SRP's testing procedure was based upon a methodology that did not unambiguously ensure information essential for recovery would in fact be tested annually to ensure its availability if recovery were necessary. The SRP testing procedure was performed annually on the control center backup media, but the testing methodology SRP used raised concerns in two areas. First, the information being stored to the media originated from six different categories of devices, but the SRP procedures required only that testing be performed on one category of device each six months. Testing one device every six months does not ensure that at least one of each category of devices will be tested annually. Under SRP's methodology, there may be an interval as long as three years between testing for any given category of device.

In addition, while SRP's methodology tested the server on which the backups resided at least annually, the sampling tested only a limited number of the essential files, making it a relatively weak indicator that the information necessary for recovery would

be available. Storage media are subject to damage that could corrupt files containing information essential to recovery. Tests that would validate the integrity of the storage media as a whole would provide a more reliable assurance that SRP's data essential for recovery would be available.

Recommendations

Audit staff recommends that SRP:

6. Consider revising its backup media testing procedures to ensure that the control center storage media themselves are more rigorously tested, and that at least one CCA from each category of assets within the control center ESP should be tested on an annual basis.

B. Operations and Planning Standards

5. Plans for Loss of Control Center Functionality

SRP did not fully test the viability of its contingency plan, which included procedures for dispatching qualified personnel to its twelve key substations to keep system operators informed of all alarms, analogs, flows, breaker operations, and operational limit violations at each substation. SRP's testing of its contingency plan was not robust, as it was based on dispatching personnel to only two of its twelve key substations.

Pertinent Guidance

EOP-008-0: Plans for Loss of Control Center Functionality

R1. 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

SRP's contingency plan included procedures for dispatching qualified personnel to key substations to keep system operators informed of, and conduct the necessary control over, all alarms, analogs, flows, breaker operations, and operational limit violations at each substation. In the event that it took more than one hour for SRP to implement its contingency plan for the loss of communications from any one of the twelve remote terminal units (RTU), an agreement between Arizona Public Service Company (APS) and SRP included provisions for APS to monitor SRP's sites in the interim.

During the audit period, SRP did not conduct a full simulation of its contingency plan related to the loss of any of these RTU communications to determine if it could operate its backup control center successfully using data from personnel dispatched to key substations. The "key" substations identified in SRP's plan include one 500-kV substation, three 115-kV substations, and eight 230-kV substations. Instead, SRP's contingency plan tested SRP's ability to dispatch staff to one or two substations to report readings and alarms. Under this plan, SRP would not be able to adequately verify that control center staff could efficiently accept the readings from one or more of these twelve RTUs.

Audit staff notes that SRP said it had plans and had purchased hardware to implement redundant communications paths to fully integrate these twelve RTUs in the EDC. SRP told audit staff during on-site interviews that its goal was to implement these upgrades by the end of 2012. However, in response to a follow-up data request after audit staff's site visit, SRP said that it postponed the complete implementation of RTU communication until 2015. Audit staff encourages SRP to implement such upgrades expeditiously. In the interim, SRP should take measures to ensure the viability of its existing contingency plan.

Recommendations

Audit staff recommends that SRP:

7. Implement its planned upgrades to RTU communications to the EDC as soon as possible.

8. If implementation of its planned upgrades to RTU communications to the EDC will take longer than six months from the date of this audit report, SRP should in the meantime develop a means to test its existing contingency plan for dispatching personnel to key substations, and conduct such a test.

6. Training for System Operators

SRP modified its training for its system operators on the characteristics of its generation resources as a result of the lessons learned during the February 2011 cold weather event. Audit staff commends SRP on its independent review, but is concerned that: (1) SRP did not conduct this training on a recurring basis; and (2) SRP did not document the attendance at and completion of initial training provided to newly hired operating personnel.

Pertinent Guidance

PER-002-0 Operating Personnel Training

> **R1.** Each Transmission Operator and Balancing Authority shall be staffed with adequately trained operating personnel . . .
> **R3.** For personnel identified in Requirement R2, the Transmission Operator and Balancing Authority shall provide a training program meeting the following criteria: . . .
>
> > **R3.2.** The training program must include a plan for the initial and continuing training of Transmission Operator and Balancing Authority operating personnel. That plan shall address knowledge and competencies required for reliable system operations.

Background

During the February 2011 cold weather event, the SRP Balancing Authority operators were not aware that their directive to return a steam turbine to service required the output of the associated combustion turbine to be reduced to minimum load. The operators directed the restart of an 80 MW steam turbine that had tripped. Restarting this steam turbine required the plant operator to reduce the output of the 159 MW gas combustion turbine to 15 MW. This restart resulted in a reduction in generating resources of 144 MW, in addition to the 80 MW lost when the steam turbine tripped.

Following the event, SRP recognized this occurrence as an issue and provided unit-specific generator characteristics training to its BA operators. However, at the time of the audit, the company had not made this training a recurring part of its training program.

Separately, audit staff notes that SRP was unable to provide detailed documentation of attendance at and completion of the classroom training provided to newly hired operating personnel that auditors would normally expect. Such detailed documentation of training provided to newly hired operating personnel is essential to

demonstrate that adequate training was provided to new operators on the use of SRP's systems, policies, and procedures.

Recommendations

Audit staff recommends that SRP:

9. Conduct a review of its training program for its operating personnel, and implement remedies to strengthen the program, including remedies that measure the effectiveness of the training provided.

10. Include training on the operating characteristics of SRP's generators as part of the recurring training for operators.

11. Develop procedures for more detailed documentation of the attendance at and completion of initial training (both classroom and on-the-job) for newly hired operating personnel.

7. Training for Distribution Operators on Load Shedding

SRP's training on load-shedding procedures for its distribution operators was more frequent as a result of lessons it learned during the February 2011 cold weather event. However, audit staff found that this training could be made more effective by including simulations and drills.

Pertinent Guidance

EOP-003-1, R8. Each Transmission Operator or Balancing Authority shall have plans for operator-controlled manual load shedding to respond to real-time emergencies. The Transmission Operator or Balancing Authority shall be capable of implementing the load shedding in a timeframe adequate for responding to the emergency.

EOP-003-1, R5. A Transmission Operator or Balancing Authority shall implement load shedding in steps established to minimize the risk of further uncontrolled separation, loss of generation, or system shutdown.

Background

Audit staff learned that during the February 2011 cold weather event, SRP's distribution operators experienced difficulty shedding load when contacted by the SRP BA operator. The load was shed, but a delay of five minutes occurred because a step was missing in the written load-shedding procedure (which was later corrected). In audit staff's view, periodic training for distribution operators that included simulations and drills may have identified the problem with the written procedures before the cold weather event occurred.

Following its review of the FERC/NERC Report on Outages and Curtailments during the Southwest cold weather event, SRP modified and augmented its load-shedding training.[8] Audit staff reviewed the updated training. The training consisted of Distribution Operations shift supervisors and dispatchers reading the load-shedding procedures twice annually. In audit staff's view, the updated training program could be enhanced by including simulations and drills, which will help ensure that load shedding is accomplished in a timely and accurate manner.

[8] FERC/NERC Staff Report on the 2011 Southwest Cold Weather Event of February 1-5, 2011: Causes and Recommendations (Aug. 2011), *available at* http://www.ferc.gov/legal/staff-reports/08-16-11-report.pdf.

Recommendations

Audit staff recommends that SRP:

12. Develop and implement training for its distribution operators that includes, at least annually, simulations and drills on load shedding and restoration. The goal of such training should be to ensure that SRP's distribution operators are capable of using the load-shedding (rotating blackout) capability of their EMS/SCADA systems.

Appendix

SRP Response to Draft Audit Report

Mail Station POB300
PO Box 52025
Phoenix AZ 85072-2025
Sara.McCoy@srpnet.com

Sara McCoy
Director
Electric Reliability Compliance
602-236-3941

June 27, 2013

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: Office of Enforcement Docket No. PA12-11-000
FERC Reliability Audit of Salt River Project Agricultural Improvement and Power District Draft Report

Dear Mr. Craig:

The Salt River Project Agricultural Improvement and Power District ("SRP") hereby submits its Response to the draft June 12, 2013 FERC Reliability Audit Report of Salt River Project Agricultural Improvement and Power District Draft Report ("Draft Report").

SRP appreciates Audit Staff's work to review extensive documentation and conduct numerous interviews of SRP staff in order to assess the SRP compliance program. As we discussed with the audit team, we continually seek opportunities to evaluate and improve our program and this audit provided another such opportunity.

As described in the audit notice, the purpose of the audit was to evaluate SRP's performance of, and compliance with, the requirements of mandatory reliability standards. The recommendations in the Draft Report address areas where performance could be enhanced. None of the recommendations identify a potential compliance concern. SRP agrees that implementation of the Draft Report recommendations will have a positive impact on the effectiveness of our compliance program.

SRP will provide a progress report on the implementation of the recommendations after the issuance of the final audit report in this docket. Many of the recommendations were already implemented following the on-site portion of the audit.

Please contact me if you have any questions.

Sincerely,

Sara McCoy

Sara McCoy

cc: Teresina Stasko - FERC
Paul Deschene - FERC
Michael Hummel - SRP
John Coggins - SRP
Margaret Rostker - SRP

Document Content(s)

PA12-11-000.PDF.....1-33