FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, D.C. 20426

In Reply Refer To:
Office of Enforcement
Docket No. PA12-17-000
April 24, 2013

John Hairston, Chief Compliance Officer
Bonneville Power Administration
P.O. Box 3621
Portland, OR 97208-3621

Dear Mr. Hairston:

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 Bonneville Power Administration (BPA), for the period from June 18, 2007, to January 25, 2013. The enclosed audit report explains our audit conclusions and recommendations.

2. The audit evaluated BPA'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. Staff initially informed BPA of the audit conclusions and recommendations in a draft audit report on March 25, 2013. Representatives from the Division of Audits and OER discussed the draft audit report with BPA on April 2, 2013. In response to the discussions, audit staff revised the draft audit report and sent it to BPA on April 5, 2013. In its April 16, 2013 response, BPA said it agrees with all audit recommendations. A copy of BPA'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, BPA should submit a plan to comply with the recommendations. BPA 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. BPA 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 Bonneville Power Administration

Docket No. PA12-17-000
April 24, 2013

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 Bonneville Power Administration (BPA or agency). The audit was commenced to evaluate BPA's compliance with the requirements of the North American Electric Reliability Corporation's (NERC) mandatory Reliability Standards pertaining to Bulk Electric System (BES) operations and planning, and Critical Infrastructure Protection (CIP). The audit covered the period from June 18, 2007 to January 25, 2013.

B. Bonneville Power Administration Overview

Based in the Pacific Northwest, BPA is a Federal nonprofit agency within the U.S. Department of Energy. One of four Federal power marketing administrations, BPA markets wholesale electric power from 31 Federal hydroelectric projects in the Columbia River Basin, one nonfederal nuclear power plant, and several small nonfederal power plants. The U.S. Army Corps of Engineers and Bureau of Reclamation operate the hydroelectric projects. BPA supplies about 30 percent of the electricity the Northwest consumes. The agency also operates and maintains about 15,000 miles of high-voltage electric transmission lines, one-third of which operates at 500 kilovolts (kV) and above. BPA transmission facilities represent three-fourths of the high-voltage (230 kV and above) transmission in its service area, which includes Idaho, Oregon, Washington, and parts of Montana, California, Nevada, Utah, and Wyoming. The agency also operates large interregional transmission lines that connect its service area to California and western Canada. BPA transmission customers include consumer- and investor-owned utilities, independent power producers, and power marketers across the western United States and the Canadian provinces of British Columbia and Alberta.

During the audit period, BPA was registered with the Western Electricity Coordinating Council Regional Entity (WECC RE) for nine reliability functions, as the NERC Functional Model[1] has defined them: Balancing Authority (BA); Load-Serving Entity (LSE); Planning Authority (PA); Purchasing-Selling Entity (PSE); Resource

[1] The NERC Reliability Functional Model defines the functions that must be performed to ensure reliability of the BES, and explains the relationships between and among the entities responsible for performing tasks within each function. The model is the foundation 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 the model.

Planner (RP); Transmission Operator (TOP); Transmission Planner (TP); Transmission Owner (TO); and Transmission Service Provider (TSP).

BPA had two control centers to carry out its registered functions: the Dittmer Control Center (DCC), in Vancouver, WA, and the Munro Control Center (MCC), in Spokane, WA. Under normal operations, the DCC was considered BPA's primary control center and performed Balancing Authority functions, such as automatic generation control, and operated all 500-kV lines plus the transmission system in the Puget Sound area. Under normal conditions, the MCC operated and controlled transmission and substation facilities below 500 kV. In the event either control center became inoperable for any reason, the other control center would take over operation and control of BPA's entire transmission system.

C. Conclusions

Audit staff found six areas in which BPA can improve compliance. A detailed discussion is provided in section III.

- *Protection Systems Maintenance and Testing:* BPA should enhance its Protection System maintenance procedures by: (1) establishing specific and supportable outer limits for maintenance and testing of all components of its Main Grid and Local Area Remedial Action Schemes (RAS), and ensuring that all deferred RAS maintenance and testing is performed before the outer limits are reached; and (2) taking all necessary actions to prevent deviations in the maintenance and testing of all Protection Systems beyond the established intervals. BPA should document in writing all instances when maintenance and testing must be deferred or is otherwise delayed beyond the outer limits. These measures will enhance the robustness of BPA's maintenance and testing program and improve the reliability of its Protection Systems.

- *Updating BPA's Equipment Tracking Tool:* BPA's process for tracking maintenance requirements should be strengthened by establishing a specific time period within which newly energized equipment must be entered into its equipment tracking tool.

- *Outage Coordination with Neighboring Entities:* BPA should improve its transmission planning procedures to ensure that information on outages of BES facilities operated by neighboring entities at less than 230 kV is accounted for when establishing system operating limits (SOLs) within the BPA system.

- *Load Shedding Plans with Distribution Providers:* BPA's load shedding plan should be improved by: (1) establishing testing criteria to ensure that distribution providers can respond to BPA's directives to shed load within the ten-minute time frame in BPA's plan; and (2) automating several of its manual processes. Such measures would enable BPA to better demonstrate its ability to meet the stated objectives of its load shedding plan.

- *Transmission Planning:* Audit staff encourages BPA to continue to assess its transmission planning study process, and make the necessary modifications to improve the efficiency and effectiveness of its long-term transmission planning.

- *Field Asset Critical Cyber Asset Identification Methodology:* BPA should develop written procedures for identifying and documenting Critical Cyber Assets where substations, field equipment, and other essential field assets are located.

D. Recommendations

Below are audit staff's recommendations to address the issues discussed in this report. Details are provided in section III.

To enhance reliability of the BES, BPA should:

1. Develop specific and supportable outer limits for the maintenance and testing intervals of all Main Grid and Local Area RAS.

2. Enhance its procedures to incorporate these outer limits when scheduling RAS maintenance and testing, and ensure all maintenance and testing is completed within these outer limits.

3. Revise its Maintenance Deviation Policy and all related documentation to specify that Protection System maintenance and testing may be deferred up to, but not beyond the outer limits of the intervals specified for the equipment.

4. Train employees on the enhanced procedures with the new intervals for Main Grid and Local Area RAS.

5. Communicate the new procedures and policies to all affected employees, including field staff.

6. Establish a specific time period within which equipment must be entered into its equipment tracking tool.

7. Revise its procedures to require all newly energized equipment to be entered into its equipment tracking tool within the established time period after it is placed in service.

8. Coordinate the inclusion of information on planned outages of BES facilities operated by neighboring entities at less than 230 kV in determining SOLs within the BPA system.

9. Implement additional tools or displays to automatically calculate load shedding allocations to distribution providers.

10. Implement additional tools or displays to automatically monitor and track the progress of distribution providers in shedding required amounts of load.

11. Consider coordinated load shedding drills with all distribution providers.

12. Continue to assess and implement changes to its transmission planning study process to ensure studies are done within the revised time frames BPA has established.

13. Create written procedures to identify field asset Critical Cyber Assets.

14. Ensure that Critical Cyber Asset identification is based not only on the Cyber Asset's ability to control a Critical Asset, but on whether the Cyber Asset performs monitoring or observation functions that could affect BES reliability.

15. Train employees on procedures describing the new field asset Critical Cyber Asset identification process.

16. Communicate the new field asset Critical Cyber Asset procedures and policies to all affected employees.

E. Implementation of Recommendations

BPA should develop an implementation plan that includes procedures for implementing this report's recommendations. The agency should submit the plan to audit staff for review within 30 days of the issuance of the final audit report in this docket. Thereafter, BPA should make nonpublic quarterly submissions to audit staff in Docket No. PA12-17-000 detailing its progress in implementing each recommended corrective action. The agency should make its nonpublic quarterly submissions no later than 30 days after the end of each calendar quarter, beginning with the first full quarter after submission of the implementation plan, and continuing until it completes all recommended corrective actions. In its submissions, BPA should include copies of any written policies and procedures developed in response to audit recommendations.

II. Introduction

A. Objectives

The audit objective was to evaluate BPA's compliance with NERC's mandatory Reliability Standards. The operations and planning Reliability Standards, which the Commission initially approved in Order No. 693, are designed to support reliable operation of the Bulk-Power System.[2] The CIP Reliability Standards, which the Commission initially approved in Order No. 706, provide a framework for identifying and protecting Critical Cyber Assets to support reliable operation of the Bulk-Power System.[3]

B. Scope and Methodology

This audit was undertaken to test BPA compliance with mandatory Reliability Standards and identify areas where BPA's transmission 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 WECC RE audits, BPA self-reported and WECC RE-alleged violations, and BES events involving BPA.

In reviewing and analyzing the agency's operations and performance, audit staff interviewed many BPA subject-matter experts. Throughout the audit, BPA readily made its experts available to address audit staff's questions and concerns. The agency's professionals were open in their discussions with audit staff, which assisted our testing and evaluations. Throughout the audit, BPA was proactive in improving its reliability and security as it learned of concerns and ways to strengthen its operations. For example, following audit staff's site visit, BPA developed a list of more than 60 items to enhance reliability and security beyond the levels required to comply with Reliability Standards.

Audit staff conferred with WECC RE throughout the audit. These discussions provided valuable information and insights, particularly given WECC RE's role as Compliance Enforcement Authority for Reliability Standards in the Western Interconnection. The collaboration included discussing BPA's reliability history,

---

[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).

reviewing WECC RE spot checks and audits that assessed BPA compliance with applicable Reliability Standards, and discussing risk areas, potential compliance violations, and areas of concern. Audit staff also conferred with other Commission staff to discuss these issues and Commission requirements relevant to them.

Audit staff performed these steps to facilitate testing and evaluation of BPA compliance and performance relevant to the audit objectives:

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

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

- *Obtained Input From Regional Entity Staff* – Audit staff contacted WECC RE staff and managers for background briefings on BPA and consultations on issues of concern.

- *Conducted Site Visits* – Audit staff conducted one site visit to BPA offices and operations facilities in Vancouver, WA. There, BPA gave audit staff presentations on major elements of BPA's reliability and cyber security programs, areas identified in audit staff's data requests, and future plans and goals for each program area. These presentations framed audit staff's interviews and discussions with BPA departments and employees, including those responsible for: (1) daily reliability operations; (2) reliability assessments; (3) monitoring, assessing threats, and managing access to BPA communication and information technology systems; (4) training and certifying employees in operations and critical infrastructure protection; and (5) overseeing compliance with Reliability Standards. BPA readily responded to audit staff's onsite requests for information and clarification, and helped audit staff's sampling and review of documents related to BPA's management and control of Critical Assets, Critical Cyber Assets, and the associated access rights to them. The visit also enabled audit staff to:

    - Obtain an overview of BPA's corporate structure, functions, and responsibilities;
    - Tour BPA's system control and data centers;
    - Interview executives, managers, and operational employees;

- Review internal audit reports;
- Review and test internal policies and procedures relevant to audit objectives; and
- Review BPA's regulatory and corporate compliance programs.

- *Interviews and Teleconferences* – Audit staff conducted numerous interviews and teleconferences with agency compliance staff, subject-matter experts, and senior managers to support audit staff's evaluation of compliance with Commission rules, regulations, and requirements.

- *Issuing Data Requests* – Audit staff issued numerous data requests to gather information. The information covered BPA's internal policies and procedures, operational data, compliance culture and compliance program documents, and documents on key policies and procedures governing BPA's performance as a NERC-registered entity responsible for certain operations, planning, and CIP standards. Audit staff used this data as a primary source for testing and evaluating compliance with Commission requirements relevant to audit objectives.

- *Providing performance improvement recommendations* – Audit staff spoke with BPA about ways to improve performance in several areas within the audit scope. These informal recommendations touched on outage planning and coordination, curtailment procedures, knowledge transfer/continuity, relay protection, cross-organizational communications, network diagrams, network security scanning, and compliance review.

Audit staff also performed testing and analysis to review the effectiveness of BPA's corporate compliance program. More specifically, audit staff tested compliance in two overarching areas: operations and planning standards, and CIP standards.

1. Operations and Planning Standards

During the audit period, BPA was registered as a Balancing Authority (BA), Load Serving Entity (LSE), Planning Authority (PA), Purchasing-Selling Entity (PSE), Resource Planner (RP), Transmission Operator (TOP), Transmission Planner (TP), and Transmission Service Provider (TSP). As such, BPA was responsible for monitoring and operating its transmission system within established operating limits, developing transmission expansion plans, and performing other reliability functions. Based on an assessment of risks related to these activities, audit staff examined and evaluated BPA's performance and compliance with NERC Reliability Standards in these functional areas:

- *Vegetation management processes and procedures*

  To verify BPA had appropriate vegetation management practices as required by the Facilities Design, Connections, and Maintenance (FAC) Standards, audit staff issued data requests and reviewed information describing the agency's Transmission Vegetation Management Plan and related procedures. Audit staff then conducted interviews and reviewed documentation to verify that BPA had properly implemented the plan.

- *Operations planning practices*

  To test that BPA had implemented operational planning practices as required by the Transmission Operations (TOP) Standards, audit staff reviewed BPA's procedures for conducting seasonal, next-day, and same-day operational planning, and interviewed managers and operational staff about these procedures. Audit staff issued data requests and conducted further interviews to clarify specific procedures. Audit staff also inspected the Dittmer Control Center to determine if the agency properly implemented its procedures.

- *Monitoring for and responding to exceedances of System Operating Limits*

  To verify that BPA had tools and procedures to monitor and respond to exceedances of System Operating Limits (SOL) as required by the TOP Standards, audit staff issued multiple data requests, interviewed BPA dispatchers, and toured the Dittmer Control Center. Audit staff also examined operational records from the control center, including responses to selected SOL exceedances on major transmission paths.

- *Long-term planning practices*

  To verify that BPA had implemented procedures to conduct long-term planning in accordance with the requirements of the Transmission Planning (TPL) Standards, audit staff issued multiple data requests and interviewed BPA's long-term planning staff. Also, audit staff reviewed long-term planning studies BPA conducted during the audit period.

- *Real and reactive power flow monitoring procedures and tools*

  To verify that BPA had procedures and tools for monitoring real and reactive power flows as required by the TOP Standards, audit staff issued data requests and reviewed documentation about agency policies and procedures for monitoring power flows in its operational area. Audit staff also interviewed BPA dispatchers and inspected control center workstations to verify the functionality of selected tools.

- *Coordination of BA and TOP functions with generators in its area*

  To verify that BPA had procedures to properly coordinate with generators in its Balancing Authority area as required by the TOP, Resource and Demand Balancing (BAL), and related Standards, audit staff issued data requests and interviewed BPA managers and operational staff. Also, audit staff tested the adequacy of BPA's coordination processes.

- *Blackstart testing plans*

  To verify that BPA had procedures to verify the feasibility of its blackstart plan as required by the Emergency Operations and Preparedness (EOP) Standards, audit staff issued data requests and interviewed BPA operational staff about the blackstart plan. Audit staff reviewed BPA's procedures for testing various elements of the plan, including simulation results and test records. Also, audit staff clarified the status of power flow and stability studies BPA had commissioned to test the blackstart plan.

- *Procedures for calculating available transmission capacity*

  To verify that BPA had procedures to properly calculate Available Transfer Capability (ATC) as required by the Modeling, Data, and Analysis (MOD) Standards, audit staff issued data requests and reviewed documents describing the design and implementation of BPA procedures for calculating ATC.

- *Staff qualifications and training*

  To verify that BPA had implemented procedures for training employees in accordance with the Personnel Performance, Training, and Qualifications (PER) Standards, audit staff issued data requests and interviewed BPA managers and dispatchers about the agency's training plan and procedures. Audit staff also reviewed BPA policies and procedures for dispatcher training, and examined operational training records on specific subjects.

- *Protective system maintenance and testing practices*

  To verify that BPA had implemented procedures to properly maintain and test protective relays and other Protection Systems as required by the Protection and Control (PRC) Standards, audit staff requested and examined documents describing BPA policies and procedures for testing Protection Systems and Special

Protection Systems, including Remedial Action Schemes. Audit staff reviewed records of transmission relay testing and interviewed BPA managers and operational staff on multiple occasions about the implementation of the agency's maintenance and testing procedures. BPA's customary practice was that, before disabling non-redundant bus differential relays on facilities rated at 115 kV and 230 kV for maintenance and testing, a BPA relay technician would first seek approval from the control center dispatcher responsible for transmission operations reliability. Then the dispatcher evaluated system conditions and made a determination as to whether the non-redundant Protection System should be disabled. In September 2012, BPA refined its procedures to require both load flow and stability studies be performed to evaluate the impact of a bus fault should it occur while the relays are disabled for testing. Audit staff reviewed the revised procedures and believes that, if properly implemented, they would provide greater assurance that BPA can safely operate its system when non-redundant relays are disabled. The agency's new procedures will strengthen BPA's maintenance program and enhance BES reliability.

2. Critical Infrastructure Protection Standards

Audit staff used a similar approach to plan and conduct its review of BPA's cyber security procedures. This portion of the audit focused on the period since WECC RE last audited BPA in October 2010. Based on reports of the U.S. Department of Energy's Inspector General, WECC RE audit reports, and a review of the most frequently violated CIP Standards, audit staff identified areas of concern to frame its initial examination. Audit staff also used observation audit experience in developing risk areas. The audit evaluated BPA procedures and processes in these areas relative to CIP Standards (using CIP Version 3 as a reference):

- *Assessment and identification of Critical Assets and associated Critical Cyber Assets*

  To verify that BPA performed a proper assessment to identify Critical Assets and associated Critical Cyber Assets, audit staff reviewed data responses, interviewed agency staff, spoke with WECC RE staff, and reviewed the OER Notice of Penalty database. Audit staff reviewed the spreadsheet BPA used to track BES equipment identified as Critical Assets. BPA used National Institute of Standards (NIST) guidelines to categorize Critical Cyber Assets and non-Critical Cyber Assets.[4] Audit staff also reviewed WECC RE open enforcement actions related to BPA's identification of Critical Assets and Critical Cyber Assets.

[4] Based in Gaithersburg, MD, NIST is the Federal agency that works with industry to develop and apply technology, measurements, and standards.

- *Electronic Security Perimeter and Physical Security Perimeter designation and protection*

  To verify that BPA had designated and implemented required controls for its Electronic Security Perimeters and Physical Security Perimeters, audit staff analyzed agency policies and procedures for designating Electronic Security Perimeters, implementing security controls, and defining and protecting its Physical Security Perimeter. Audit staff then reviewed data responses, interviewed agency staff, and inspected selected Electronic Security Perimeters and Physical Security Perimeters during a site visit. Also, audit staff reviewed remote access policies and controls for access to BPA's Electronic Security Perimeters.

- *Training, personnel risk assessment, and access control policies, procedures, and controls related to Critical Cyber Assets*

  To verify that BPA had effective access control policies and procedures for Critical Cyber Assets, audit staff reviewed the agency's training program and checked that it included all required materials. To test that BPA had completed risk assessments prior to granting personnel access to protected facilities and had effective access control mechanisms, audit staff reviewed data responses and interviewed agency employees. Audit staff also sampled records to ensure access was appropriately granted to BPA employees and contractors.

- *System security management policies, procedures, and controls related to Critical Cyber Assets*

  To verify that BPA had effective system security management procedures, audit staff conducted background research, issued data requests, and interviewed BPA staff. Audit staff examined policies and procedures related to change and configuration management, vulnerability assessment, testing, and ports and services to determine if BPA had specific, defined policies and procedures for each subject area.

- *Critical Cyber Asset recovery plans*

  To verify that BPA had documented recovery plans for its Critical Cyber Assets, audit staff reviewed agency policies and procedures describing how BPA exercised and updated its recovery plans for each class of Critical Cyber Assets, as needed. Audit staff reviewed data responses and interviewed employees to clarify how BPA implemented the plans.

III. Conclusions and Recommendations

A. Operations and Planning Standards

1. Protection System Maintenance and Testing

BPA should enhance its Protection System maintenance procedures by: (1) establishing specific and supportable outer limits for maintenance and testing of all components of its Main Grid and Local Area Remedial Action Schemes (RAS), and ensuring that all deferred RAS maintenance and testing is performed before the outer limits are reached; and (2) taking all necessary actions to prevent deviations in the maintenance and testing of all Protection Systems beyond the established intervals. BPA should document in writing all instances when maintenance and testing must be deferred or is otherwise delayed beyond the outer limits. These measures will enhance the robustness of BPA's maintenance and testing program and improve the reliability of its Protection Systems.

Pertinent Guidance

Reliability Standard PRC-005-1b states:

> R1. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the BES. The program shall include:
>
> R1.1. Maintenance and testing intervals and their basis.
>
> R1.2. Summary of maintenance and testing procedures.
>
> R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:
>
> R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.
>
> R2.2. Date each Protection System device was last tested/maintained.

Reliability Standard PRC-017-0 states in pertinent part:

> R1. The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall have a system maintenance and testing program(s) in place. The program(s) shall include:
>
> R1.2. Documentation of maintenance and testing intervals and their basis.
> R1.3. Summary of testing procedure.
> R1.4. Schedule for system testing.
> R1.5. Schedule for system maintenance.
> R1.6. Date last tested/maintained.

BPA System Protection Control Equipment Maintenance Interval Standard (STD-MC-R00016-01) states in pertinent part:

> This standard describes the Maintenance intervals associated with each System Protection & Control (SPC) Equipment Type. BPA's protective relay maintenance intervals were determined by the System Protection and Control Functional Team. The intent is to use the longest intervals (lowest frequency of maintenance) that the Functional Team has confidence will not diminish the reliability and security of the protective relays or other protection and control equipment. Maintenance completed within this time [the maintenance due date] is considered on-time and meets the requirements of the Maintenance Program. Maintenance that is not completed within 25% of the maintenance interval after the target date is past due and subject to sanctions by WECC.

BPA's Work Standard X.O-1 Maintenance Interval Deviation General Policy states in pertinent part:

> It is Transmission's policy to annually plan, implement, document and certify BPA's Transmission Maintenance and Inspection Plan, Protective Systems Maintenance and Testing Program, and Transmission Vegetation Maintenance Program and other maintenance and testing programs, consistent with WECC and NERC Standards and Requirements.
>
> It is also Transmission's policy to provide a standard means to evaluate, document, and approve maintenance deviations where warranted. Task and work order deviations considered under this policy will be evaluated on an individual basis.
>
> The due date is the last date on which a maintenance task or work order can be completed without a violation.

Within Transmission, deviations consisting of maintenance deferrals beyond the due date may be authorized for individual tasks only by the Equipment Specialist in technical service.

Deviations shall be requested:

- By the District Engineer, Foreman, District Manager or Equipment Specialist in technical service,
- Typically in advance of the target date to allow time for review and approval before the due date is reached,
- Due to an appropriate safety or business reason.

Background

During the audit period, BPA operated many Protection Systems designed to ensure the reliability of its transmission system. Protection System components include protective relays and associated communication systems, voltage and current-sensing devices, station batteries, and direct current control circuitry. Special classes of protection systems, termed Remedial Action Schemes (RAS), are designed to respond automatically when their sensors detect predetermined or abnormal system conditions. An automated response may include changing load, generation, or system configuration to maintain system stability. During the audit period, BPA had both Main Grid RAS, which were large and impacted main transmission paths, and Local Area RAS with local impacts.[5]

Reliability Standards PRC-005-1b and PRC-017-1 require TOs to have maintenance and testing programs for all Protection Systems and Special Protection Systems they own that affect BES reliability. Maintenance programs must specify maintenance and testing intervals for Protection Systems and Special Protection Systems, provide the basis for those intervals, and document that maintenance was performed according to the intervals. The purpose of these Standards is to establish outer limits for performing maintenance and testing. Registered entities may establish more frequent intervals operationally, but the standards are written to prevent entities from operating beyond the outer limits of the required intervals they establish.

To demonstrate its compliance with these Reliability Standards, BPA gave audit staff two internal standards that specified maintenance and testing intervals for relays, Protection Systems, and Special Protection Systems.[6] BPA used these standards to

---

[5] The terms Main Grid RAS and Local Area RAS fall under the NERC definition of Special Protection Systems (SPS) and are subject to compliance with PRC-017-1.

[6] SPC Equipment Maintenance Interval Standard (STD-MC-R00016-01) provided maintenance intervals for all relays and related elements on the BPA system. Relay Maintenance and Installation Testing Standard (S R RLYTST-1) documented BPA test

establish its maintenance and testing intervals, i.e., the allowable time between maintenance and testing, for each piece of Protection System equipment it owned. Also, BPA provided a third internal standard describing its Maintenance Deviation Policy.[7]

Remedial Action Scheme Maintenance and Testing Intervals

During fieldwork, audit staff discovered that BPA had not established specific and supportable maintenance and testing intervals for either Main Grid or Local Area RAS. BPA relied on its SPC Equipment Maintenance Interval Standard, which stated that Main Grid and Local Area RAS were to be tested "as required." BPA's internal documentation for RAS maintenance and testing provided context for the "as required" terminology.[8] This documentation indicated that BPA normally conducted maintenance and testing of Main Grid RAS annually, although this timeframe could be extended to 18 months and beyond if system conditions warranted.

Audit staff believes that annual maintenance and testing would contribute to a high level of reliability and meet the requirements of the Standards if carried out in practice. However, BPA's documents did not establish an outer limit for the maintenance and testing intervals for Main Grid or Local Area RAS, or a basis for the current annual to 18-month limit, other than that it was BPA's customary practice. This introduced ambiguity as to the extent to which maintenance could be deferred under BPA's applicable documents. BPA's procedures could be enhanced by addressing this ambiguity.

Audit staff believes BPA could establish a more robust maintenance and testing program and operate its Protection Systems more reliably by providing specific and supportable outer limits for the maintenance and testing intervals for Main Grid and Local Area RAS. This change would give maintenance personnel firm deadlines to use in planning the numerous maintenance and tests required, and help verify that BPA staff performed the tests in a timely manner.

Maintenance Deviations

Besides the special procedures for RAS, BPA allowed maintenance staff to request a deviation or extension of planned maintenance and testing for all Protection Systems beyond the established maintenance interval "due to an appropriate safety or business reason." Under BPA Work Standard X.O-1, the deviation policy provides a "standard means for BPA to identify, reclassify, document, and track individual tasks and work

---

requirements for commissioning new relays and for routine relay maintenance.

[7] BPA Work Standard X.O-1 Maintenance Interval Deviation General Policy (Maintenance Deviation Policy).

[8] RAS Documentation of Maintenance and Testing Intervals and Their Basis, September 28, 2011.

orders that cannot or should not be completed on schedule." The district engineer and foreman evaluated the requests, which the equipment specialist in the technical services department approved. BPA policy described several instances in which a deviation could be appropriate, but did not place any limits on the use of deviations, or identify boundaries beyond which BPA would not permit deviations.

Audit staff is concerned that BPA's deviation policy effectively placed no limits on the number or length of deviations from maintenance and testing intervals BPA staff could obtain. The fact that "business reasons" could be used to grant deviations heightens these concerns. While audit staff found no evidence that, in practice, cumulative deviations have threatened reliability to date, controls to prevent this from occurring were lacking in BPA's documented procedures.

Audit staff believes BPA should enhance its procedures by specifying outer limits beyond which it would not permit deviations from established maintenance and testing intervals. Audit staff also encourages the agency to document all instances when maintenance or testing must be deferred or delayed beyond the outer limits.

Recommendations

We recommend that BPA:

1. Develop specific and supportable outer limits for the maintenance and testing intervals of all Main Grid and Local Area RAS.

2. Enhance its procedures to incorporate these outer limits when scheduling RAS maintenance and testing, and ensure all maintenance and testing is completed within these outer limits.

3. Revise its Maintenance Deviation Policy and all related documentation to specify that Protection System maintenance and testing may be deferred up to, but not beyond the outer limits of the intervals specified for the equipment.

4. Train employees on the enhanced procedures with the new intervals for Main Grid and Local Area RAS.

5. Communicate the new procedures and policies to all affected employees, including field staff.

2. Updating BPA's Equipment Tracking Tool

BPA's process for tracking maintenance requirements should be strengthened by establishing a specific time period within which newly energized equipment must be entered into its equipment tracking tool.

Pertinent Guidance

Reliability Standard PRC-005-1b states:

> R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:
>
> > R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.
> >
> > R2.2. Date each Protection System device was last tested/maintained.

Background

During the audit, audit staff discovered that several pieces of equipment were missing from the list BPA used to track maintenance and testing of Protection Systems. Staff found that several devices had not been added to the list even though they had been placed in service nearly six months earlier. An incomplete list could lead to an inadequate maintenance and testing schedule, which could impact BES reliability. Based on a review of the list, audit staff found that the difficulties largely stemmed from BPA's process for entering newly energized equipment into its tracking software.

BPA used its Cascade software application as its primary tool for maintaining an inventory of transmission facilities and planning equipment maintenance and testing. Agency field staff entered data on newly energized equipment into Cascade after the equipment had been installed. Information entered into Cascade included the date the equipment was energized or placed in service, and the date it was listed in Cascade. BPA used the date the equipment was energized to schedule maintenance, which ensured maintenance was performed within the appropriate maintenance interval.

However, BPA's procedure did not prescribe a deadline for entering information into Cascade. Audit staff believes this omission created a possibility that data on newly energized equipment would not be entered in a timely manner, which could disrupt the agency's relay maintenance processes. At the very least, lack of a deadline for entering this information could cause an incomplete list of equipment required to be maintained and tested. To mitigate this risk and ensure equipment lists are current, BPA should revise its procedures to require all equipment to be entered into Cascade within an appropriate timeframe after it is placed in service. Audit staff noted that BPA is already working to improve this process.

Recommendations

We recommend that BPA:

6. Establish a specific time period within which equipment must be entered into its equipment tracking tool.

7. Revise its procedures to require all newly energized equipment to be entered into its equipment tracking tool within the established time period after it is placed in service.

3. Outage Coordination with Neighboring Entities

BPA should improve its transmission planning procedures to ensure that information on outages of BES facilities operated by neighboring entities at less than 230 kV is accounted for when establishing system operating limits (SOLs) within the BPA system.

Pertinent Guidance

Reliability Standard TOP-002-2.1b states:

> R6. Each Balancing Authority and Transmission Operator shall plan to meet unscheduled changes in system configuration and generation dispatch (at a minimum N-1 Contingency planning) in accordance with NERC, Regional Reliability Organization, subregional, and local reliability requirements.
>
> R11. The Transmission Operator shall perform seasonal, next-day, and current-day Bulk Electric System studies to determine SOLs. Neighboring Transmission Operators shall utilize identical SOLs for common facilities. The Transmission Operator shall update these Bulk Electric System studies as necessary to reflect current system conditions; and shall make the results of Bulk Electric System studies available to the Transmission Operators, Balancing Authorities (subject to confidentiality requirements), and to its Reliability Coordinator.

Reliability Standard TOP-004-2 states:

> R1. Each Transmission Operator shall operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs).
>
> R2. Each Transmission Operator shall operate so that instability, uncontrolled separation, or cascading outages will not occur as a result of the most severe single contingency.

Background

TOP-002-2.1b R11 requires BPA, as the Transmission Operator, to perform system studies to determine SOLs within its system, and update these studies as needed to reflect current system conditions. BPA conducts the studies required by TOP-002-2.1b

R11 in conjunction with other members of the Northwest Power Pool (NWPP).[9] Information on planned outages of transmission facilities is a key input into the studies. In performing the studies, BPA's operations planning engineers worked closely with other members of the NWPP to evaluate the impact of planned equipment outages 45 days before the planned outage is to begin. This process helped ensure timely, accurate communication about upcoming outages within the regional transmission system.

Under the outage coordination process used by the NWPP, planned outages of NWPP members' BES facilities operated at or above 230 kV were included in the system studies BPA used to determine SOLs. However, facilities below 230 kV were included only if the facility owner or operator believed their inclusion would provide information helpful to itself or other participants, or if all other NWPP members asked that the facility be included.

Based upon discussions with BPA employees, audit staff determined that BPA studied the impacts of planned outages of all BPA-owned BES facilities operating at 115 kV and above in determining the SOLs of its transmission paths. However, not all NWPP members provided information on planned outages of BES facilities operated at less than 230 kV.

Audit staff is concerned that omitting the impact of such outages could reduce the accuracy of BPA's studies to determine SOLs within the BPA system.[10]

Recommendation

We recommend that BPA:

8. Coordinate the inclusion of information on planned outages of BES facilities operated by neighboring entities at less than 230 kV in determining SOLs within the BPA system.

---

[9] NWPP is a voluntary organization comprised of major generating utilities serving the Northwestern United States, British Columbia and Alberta. Transmission operators in the Pacific Northwest voluntarily participate in an outage planning process wherein NWPP members provide information regarding planned transmission outages. Each individual transmission operator then performs its own studies using the outage information to determine SOLs on its transmission paths. The NWPP itself does not perform studies to determine SOLs.

[10] BPA should review the need to incorporate facilities operating at voltages below 100 kV into its SOL determinations. Consideration of sub-100 kV facilities in setting SOLs was a major finding of the April 2012 Joint FERC and NERC inquiry into the September 8, 2011 Arizona-Southern California Blackout. *See FERC/NERC Staff Report on the September 8, 2011 Blackout* at 96-97.

4. Load Shedding Plans with Distribution Providers

BPA's load shedding plan should be improved by: (1) establishing testing criteria to ensure that distribution providers can respond to BPA's directives to shed load within the ten-minute timeframe in BPA's plan; and (2) automating several of its manual processes. Such measures would enable BPA to better demonstrate its ability to meet the stated objectives of its load shedding plan.

Pertinent Guidance

Reliability Standard EOP-003-1 states:

> 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.

Reliability Standard VAR-001-2 states:

> R12. The Transmission Operator shall direct corrective action, including load reduction, necessary to prevent voltage collapse when reactive resources are insufficient.

WECC Regional Reliability Standard TOP-007-WECC-1 states:

> R1. When the actual power flow exceeds an SOL for a Transmission path, the Transmission Operators shall take immediate action to reduce the actual power flow across the path such that at no time shall the power flow for the Transmission path exceed the SOL for more than 30 minutes.

Background

High power flows on the transmission system can lead to a drop in voltage on the transmission system. If voltage falls too low, it can potentially cause cascading outages that could create a widespread blackout across large areas of the transmission system.

One way to raise voltage and prevent the possibility of cascading outages is by shedding load, i.e., disconnecting customers to reduce demand and thereby reduce power flows on the transmission system. Shedding load is typically an option of last resort and generally reserved for emergencies when electricity flows exceed the reliable limits needed to maintain normal voltage. In the event of abnormally high flows on certain portions of BPA's system, BPA operators may have limited time to shed load in order to avoid potential cascading outages and a resulting widespread blackout.

During the audit period, BPA's system had several areas prone to voltage stability issues under specific conditions. Of particular concern were the greater Portland, OR, and Seattle, WA, areas. During the winter, these regions were susceptible to voltage collapse due to the high electricity demand. Should flows exceed reliable limits near Portland and Seattle, timely load shedding could mean the difference between a controlled, temporary loss of service for a relatively small number of customers, and a more significant outage.

BPA Load Shedding Procedures

BPA's load shedding procedures for the transmission paths serving these regions required the dispatcher to calculate the amount of load relief needed to bring electricity flow within reliable operating limits. Based on this calculation, BPA prorated load relief responsibility to each distribution provider in the affected area.

The allocation was accomplished by manually calculating the amount of load relief required from each distribution provider using a spreadsheet tool at the BPA dispatcher's workstation. The dispatcher then called each affected distribution provider and directed it to shed the specified amount of load within 10 minutes. During the site visit, BPA dispatchers told audit staff that if the distribution provider did not shed load within the allotted time, BPA would shed load at the transmission level as necessary. BPA would accomplish this by opening the high-side breaker on the step-down transformer, effectively dropping all customers connected to the low side of the transformer. However, doing so was generally undesirable because it would disconnect all customers in the affected area, including critical loads such as emergency responders and hospitals.[11]

Under TOP-007-WECC-1, load shedding, or other alternative measures, must be used to bring transmission paths within limits in 30 minutes or less after an SOL is exceeded. Audit staff believes that, if implemented properly, BPA dispatch procedures would enable it to shed load within the time frame required by TOP-007-WECC-1. However, BPA had not conducted any drills or training exercises to verify that its procedures, and the actions distribution providers took in response to them, could achieve the agency's stated objective of shedding load in 10 minutes or less.

Audit staff believes BPA should make several improvements to increase the efficiency and effectiveness of its load shedding procedures. First, BPA should consider

[11] Audit staff notes that BPA did not have to perform load shedding during the audit period.

automating the process of determining the amount of load each distribution provider must shed during an emergency, e.g., by integrating the current manual spreadsheet tool into BPA's Energy Management System. This automation would likely reduce the time needed to calculate the amount of load shedding required of each distribution provider. We are encouraged that BPA has taken steps since the site visit to address our concerns on this point.

Second, BPA should consider automating its process for tracking the amount of load distribution providers actually shed. During the audit period, BPA manually totaled the load on each distribution provider's feeder lines to determine if it had shed the required amount of load. Automating this process may provide quicker feedback, improve situational awareness of distribution providers' load shedding efforts, and alert BPA to the need to open transmission breakers if distribution providers' load shedding is inadequate or too slow.

Finally, BPA should consider conducting joint drills or training exercises with distribution providers to ensure the staffs of BPA and distribution providers thoroughly understand the load shedding procedures and can implement them within the ten-minute time frame. Audit staff notes that the agency held a limited scope training session with two distribution providers to familiarize them with how their actions fit into the load shedding process. Such sessions should be expanded to joint drills or tabletop exercises involving all critical distribution providers. BPA told audit staff it is evaluating the feasibility of enhancing its training and load shedding procedures by working with distribution providers.

Recommendations

We recommend that BPA:

9. Implement additional tools or displays to automatically calculate load shedding allocations to distribution providers.

10. Implement additional tools or displays to automatically monitor and track the progress of distribution providers in shedding required amounts of load.

11. Consider coordinated load shedding drills with all distribution providers.

Corrective Actions

Based on audit staff recommendations, BPA has improved its tools for load shedding. The agency added a load drop calculator to its Energy Management System that allows dispatchers to input the total amount of load relief required in MW. The display automatically calculates each distribution provider's MW share of the load shed, with adjustments for winter and summer conditions. This implements Recommendation No. 9.

5. Transmission Planning

Audit staff encourages BPA to continue to assess its transmission planning study process, and make the necessary modifications to improve the efficiency and effectiveness of its long-term transmission planning.

Pertinent Guidance

Reliability Standard TPL-001-0.1 states in pertinent part:

> R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that, with all transmission facilities in service and with normal (pre-contingency) operating procedures in effect, the Network can be operated to supply projected customer demands and projected Firm (non- recallable reserved) Transmission Services at all Demand levels over the range of forecast system demands, under the conditions defined in Category A of Table I.

Reliability Standard TPL-002-0b states in pertinent part:

> R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is planned such that the Network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand levels over the range of forecast system demands, under the contingency conditions as defined in Category B of Table I.

Reliability Standard TPL-003-0a states in pertinent part:

> R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission systems is planned such that the network can be operated to supply projected customer demands and projected Firm (non-recallable reserved) Transmission Services, at all demand Levels over the range of forecast system demands, under the contingency conditions as defined in Category C of Table I (attached). The controlled interruption of customer Demand, the planned removal of generators, or the Curtailment of firm (non-recallable reserved) power transfers may be necessary to meet this standard.

Reliability Standard TPL-004-0 states in pertinent part:

> R1. The Planning Authority and Transmission Planner shall each demonstrate through a valid assessment that its portion of the interconnected transmission system is evaluated for the risks and consequences of a number of each of the extreme contingencies that are listed under Category D of Table I.

Background

Transmission planning involves the use of computer models to study the performance of the electric transmission system under various future demand conditions. These simulations include power flow or load flow studies, and stability studies.

Load flow studies represent the power system at a single moment in time, and are generally used for detecting voltage deviations outside normal limits and flows above facility ratings. Stability studies simulate the operation of the power system over a period of time, generally a few seconds, to examine the impact of a potential disturbance on voltage, frequency, and other variables. Unlike load flow studies, stability studies are able to predict whether the system will remain stable after a disturbance. By performing these studies, transmission planners can identify deficiencies in the performance of the system and evaluate potential solutions such as building additional facilities. Study results are used to identify system performance deficiencies and related corrective plans under the TPL standards.

The first step in BPA's planning process was a screening study the agency performed every three years. The screening study provided a full load flow and stability study of the agency's entire transmission system, which it used to identify areas with deficient performance that need further study.[12]

In performing the study, BPA system planners used the latest WECC approved 5- and 10-year base cases for winter and summer. The base cases were the starting point for more detailed assessments of system performance under different scenarios such as winter peak, summer peak, and light load conditions. Besides power flow studies, BPA conducted more detailed stability analyses of the most critical system conditions.

[12] The level of system performance required for a particular type of contingency is explained in Table I of the TPL standards. Examples of "deficient" system performance include excessively high or low voltage, facilities operating beyond designed ratings, system instability, and cascading outages.

For each area in which it identified deficient performance, BPA performed a detailed area study that primarily examined sensitivities related to load and generation in the area. These studies included a review of historical data to ensure the parameters used were valid. Based on these studies, BPA developed corrective plans to achieve required level of system performance. Corrective plans generally included facility modifications or new operating procedures.

Audit staff understands that BPA's screening study could take nearly nine months to complete. This meant that areas not identified for additional detailed analysis by the screening study might not be examined again for nearly three years. Audit staff is concerned that during this time, system conditions in an area could change such that the transmission system may no longer meet the required level of performance.[13]

While BPA monitored significant changes in system conditions, audit staff believes additional enhancements to the agency's processes would be beneficial. These enhancements could ensure that significant changes in system conditions are detected and, to the extent they create unacceptable levels of system performance, addressed with corrective action plans.

BPA has taken steps to address audit staff's concerns. Starting in 2013, the agency will no longer conduct a preliminary screening study. Instead, BPA will review all load service areas in its footprint annually for changes in loads, generation, or transmission topology since the last study. Areas with significant changes, such as new generation or higher than expected load growth, will receive a detailed study. For an area with no significant changes, but where system upgrades are planned in the next two to five years, BPA will study the most critical contingencies for that area using the latest available information to ensure planned upgrades still achieve the needed levels of performance. Areas with no significant changes since the last study and no planned upgrades within the next two to five years will be studied at least every two years.

These enhancements ensure that each load area in BPA's system will be studied at least every two years as opposed to every three years under the current procedure. Audit staff believes BPA's revised study process represents a significant improvement. Audit staff encourages BPA to continue implementing these changes to improve both the effectiveness and efficiency of its long-term planning process.

---

[13] For example, if an area experienced higher-than-expected load growth and a long-term transmission or generation outage, power flows could exceed facility ratings on some lower voltage transmission lines.

Recommendation

We recommend that BPA:

12. Continue to assess and implement changes to its transmission planning study process to ensure studies are done within the revised time frames BPA has established.

B. Critical Infrastructure Protection Standards

1. Field Asset Critical Cyber Asset Identification Methodology

BPA should develop written procedures for identifying and documenting Critical Cyber Assets where substations, field equipment, and other essential field assets are located.

Pertinent Guidance

Reliability Standard CIP-002-3 states:

> 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. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> R3.2. The Cyber Asset uses a routable protocol within a control center; or,
>
> R3.3. The Cyber Asset is dial-up accessible.

NERC Security Guideline for Identifying Critical Cyber Assets states:

> A Cyber Asset could be considered essential to the reliable operation of a Critical Asset, if one or more of the following criteria is met: (1) The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset, (2) The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset, or (3) The Cyber Asset fulfills another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BPS.[14]

---

[14] Security Guideline for the Electricity Sector: Identifying Critical Cyber Assets (June 17, 2010), *available at*

Background

BPA used two separate methodologies for determining its list of Critical Cyber Assets: one for control center assets, the other for field assets. The agency gave two reasons for using a two-pronged approach. First, Cyber Assets at substations tended to be device-centric, whereas Cyber Assets at control centers were organized into discrete information systems. Also, BPA's organizational structure divided responsibility for identifying Critical Cyber Assets between two organizations – Transmission Operations for control centers and Transmission Engineering for substations and other field assets.

BPA used a well-defined process to identify Critical Cyber Assets in control centers. BPA based the identification on the criteria specified in Federal Information Processing Standard (FIPS) 199 and the steps outlined in National Institute of Standards and Technology Special Publication 800-60. As a Federal entity, BPA must comply with the Federal Information Security Management Act, of which FIPS is part.

However, in the field environment, BPA did not have a clearly defined process for identifying Critical Cyber Assets. Standard CIP-002-3 R3 explicitly requires a responsible entity to develop a list of Critical Cyber Assets essential to the operation of each Critical Asset, although it does not prescribe that a specific process be documented. While not having written procedures does not directly affect reliability or security, failure to identify all Critical Cyber Assets that should be identified could have an adverse impact, particularly if the unidentified Critical Cyber Assets are not protected by appropriate protective, preventive, and detective controls.

BPA should develop documented procedures for field asset Critical Cyber Asset identification so it can: (1) consistently identify Critical Cyber Assets in compliance with CIP-002 R3 in Version 3 and later versions; (2) ensure that future assets (e.g., new substations) are properly evaluated for Critical Cyber Assets; (3) improve coordination between the two groups responsible for identifying Critical Cyber Assets; and (4) use current employees' expertise to train new ones in Critical Cyber Asset identification. In preparation for CIP Version 4, which is currently scheduled to replace Version 3, audit staff recommends that BPA develop a Critical Cyber Asset identification process for field asset devices. Audit staff believes that the "bright line" criterion specified in CIP-002 Version 4 will require BPA to identify additional Critical Assets that it has not identified under previous versions of this Standard. The agency will need to evaluate these newly identified Critical Assets in updating its list of Critical Cyber Assets.

---

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.

Also, BPA explained that it considered Critical Cyber Assets as those essential to the control of the Critical Asset.[15] Control and operation have different meanings, and BPA should modify its procedures to ensure that control is not the sole criterion used to identify Critical Cyber Assets. In identifying whether a Cyber Asset is essential to the operation of a Critical Asset, audit staff encourages BPA to consider not only control capability, but whether the Cyber Asset performs monitoring or observation functions that could affect BES reliability.

NERC guidance reiterates this point:

> A Cyber Asset could be considered essential to the reliable operation of a Critical Asset, if one or more of the following criteria is met: (1) The Cyber Asset participates in, or is capable of, supervisory or autonomous control that is essential to the reliable operation of a Critical Asset, (2) The Cyber Asset displays, transfers, or contains information relied on to make Real-time operational decisions that are essential to the reliable operation of a Critical Asset, or (3) The Cyber Asset fulfills another function essential to the reliable operation of the associated Critical Asset and its Loss, Degradation, or Compromise would affect the reliability or operability of the BPS.

Written procedures for Critical Cyber Asset identification will be especially important in helping BPA prepare for compliance with CIP Version 4. The agency has already identified some 30 additional Critical Asset substations it needs to evaluate for Critical Cyber Assets under CIP Version 4. Developing explicit written procedures would require BPA to define the type of equipment it considers essential to operation of a Critical Asset substation – an area audit staff discovered BPA had not documented. Also, audit staff noted that BPA has developed field equipment policies and procedures for other CIP requirements, and recommends the same rigor be applied to Critical Cyber Asset identification that triggers compliance obligations pursuant to other CIP requirements. Lastly, such a proactive approach to specifying field equipment may prevent confusion or application of an inappropriate procedure.

Recommendations

We recommend that BPA:

13. Create written procedures to identify field asset Critical Cyber Assets.

14. Ensure Critical Cyber Asset identification is not based only on the Cyber Asset's ability to control a Critical Asset, but on whether the Cyber Asset

[15] BPA's internal definition of "essential" as it pertains to substations, provided in audit data responses.

performs monitoring or observation functions that could affect BES reliability.

15. Train employees on procedures describing the new field asset Critical Cyber Asset identification process.

16. Communicate the new field asset Critical Cyber Asset procedures and policies to all affected employees.

Appendix

BPA Response to Draft Audit Report

Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

April 16, 2013

In reply refer to: DG-7

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: Docket No. PA12-17

Dear Mr. Craig:

Bonneville Power Administration (BPA) provides the following response to the Draft Audit Report of the Division of Audits and the Office of Enforcement of the Federal Energy Regulatory Commission (FERC) related to BPA's compliance with mandatory reliability standards conducted pursuant to Docket No. PA12-17.

Recommendation 1: Develop specific and supportable outer limits for the maintenance and testing intervals of all Main Grid and Local Area RAS.

BPA agrees with Recommendation 1. BPA has not completed corrective actions for this recommendation. BPA will develop corrective actions and a target completion date for inclusion in the implementation plan that will be submitted to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 2: Enhance its procedures to incorporate these outer limits when scheduling RAS maintenance and testing, and ensure all deferred maintenance and testing is expedited to stay within these outer limits.

BPA agrees with Recommendation 2. BPA has not completed corrective actions for this recommendation. BPA will develop corrective actions for inclusion in the implementation plan that it will submit to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 3: Revise its Maintenance Deviation Policy and all related documentation to specify that Protection System maintenance and testing may be deferred up to, but not beyond the outer limits of the intervals specified for the equipment.

BPA agrees with Recommendation 3. BPA has not completed corrective actions for this recommendation. BPA has identified and will begin the following corrective actions: initiate cross-organizational discussions to investigate maintenance practices as they relate to outages; discuss options for arranging a maintenance deviation process between BPA and WECC; and revise the policy based on the outcome of the aforementioned corrective actions. A target completion date has not yet been determined.

Recommendation 4: Train employees on the enhanced procedures with the new intervals for Main Grid and Local Area RAS.

BPA agrees with Recommendation 4. BPA has not completed corrective actions for this recommendation. BPA will develop corrective actions for inclusion in the implementation plan that it will submit to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 5: Communicate the new procedures and policies to all affected employees, including field staff.

BPA agrees with Recommendation 5. BPA has not completed corrective actions for this recommendation. BPA will evaluate the required actions to ensure adequate communications of any newly developed policies and procedures arising from the supporting recommendations. The cross-organizational efforts of the supporting recommendations will dictate the delivery dates for this recommendation. A target completion date has not yet been determined.

Recommendation 6: Establish a specific time period within which equipment must be entered into its equipment tracking tool.

BPA agrees with Recommendation 6. As stated in the report, BPA is already working to improve this process. BPA has begun planning for how to address this recommendation. This recommendation will be addressed as part of a BPA Data Oversight and Delivery project. We will evaluate the process for entering equipment into the equipment tracking tool, including the determination of a specific time period and revision of procedures supporting the equipment entry into the equipment tracking tool. A target completion date has not yet been determined.

Recommendation 7: Revise its procedures to require all newly energized equipment to be entered into its equipment tracking tool within the established time period after it is placed in service.

BPA agrees with Recommendation 7. As stated in the report, BPA is already working to improve this process. BPA has begun planning for how to address this recommendation. This recommendation will be addressed as part of a BPA Data Oversight and Delivery project. We will evaluate the process for entering equipment into the equipment tracking tool, including the determination of a specific time period and revision of procedures supporting the equipment entry into the equipment tracking tool. A target completion date has not yet been determined.

Recommendation 8: Coordinate the inclusion of information on planned outages of BES facilities operated by neighboring entities at less than 230 kV in determining SOLs within the BPA system.

BPA agrees with Recommendation 8. In developing SOLs, BPA includes information on planned outages of impacting facilities that operate at less than 230 kV. The facilities included are not only BPA-owned equipment but impacting facilities and equipment owned by other Northwest Power Pool (NWPP) members and neighboring Transmission Operators.

Since the FERC on-site visit, BPA has taken the following actions through its membership in the NWPP. BPA, as the facilitator for the NWPP voluntary outage coordination process, has played an active roll in promoting proper outage coordination among all NWPP members. BPA is participating with other NWPP members in the NWPP outage coordination task force. This committee is tasked with developing an outage coordination process that includes all BES facilities (including those that operate at less than 230 kV) and that meets the needs of all NWPP members.

BPA will develop additional corrective actions for inclusion in the implementation plan that it must submit to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 9: Implement additional tools or displays to automatically calculate load shedding allocations to distribution providers.

BPA agrees with Recommendation 9. As noted by FERC on page 24 of its audit report, "BPA has improved its tools for load shedding. The agency added a load drop calculator to its Energy Management System that allows dispatchers to input the total amount of load relief required in MW. The display automatically calculates each distribution provider's MW share of the load shed, with adjustments for winter and summer conditions. This implements Recommendation No. 9."

BPA's manual calculation of load shedding is used as a last resort if BPA must shed load to respond to real-time emergencies. Manual calculations would be performed only if BPA's automated tool is unavailable.

All corrective actions have been completed.

Recommendation 10: Implement additional tools or displays to automatically monitor and track the progress of distribution providers in shedding required amounts of load.

BPA agrees with Recommendation 10. BPA has not completed corrective actions for this recommendation. BPA will develop corrective actions for inclusion in the implementation plan that it will submit to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 11: Consider coordinated load shedding drills with all distribution providers.

BPA agrees with Recommendation 11. BPA has not completed corrective actions for this recommendation. BPA will develop corrective actions for inclusion in the implementation plan that it will submit to FERC within 30 days after issuance of the final audit report. A target completion date has not yet been determined.

Recommendation 12: Continue to assess and implement changes to its transmission planning study process to ensure studies are done within the revised timeframes BPA has established.

BPA agrees with Recommendation 12. BPA implemented changes in 2013 to address this recommendation. BPA began performing annual assessments; these assessments review changes in loads, generation, or transmission topology across BPA's system. BPA's new process is that, based on these assessments, detailed studies will be performed for areas with significant changes to ensure the planned changes are still appropriate. BPA will also perform studies for areas which did not have significant changes, but where system upgrades are planned within the next two to five years, in order to ensure that the planned upgrades are still appropriate. Finally, for areas without planned upgrades or significant changes, detailed studies will be performed at least every two years. Transmission Planning also continues to assess its processes and make necessary modifications to improve the efficiency and effectiveness of its long-term planning.

All corrective actions have been completed.

Recommendation 13: Create written procedures to identify field asset CCAs.

BPA agrees with Recommendation 13. BPA has previously identified this area for improvement and developed a plan to create, document, and apply a combined Critical Cyber Asset identification methodology to assets in BPA's control centers and field locations. The new CCA identification methodology is expected to be complete by May 15, 2013.

Recommendation 14: Ensure that CCA identification is based not only on the Cyber Asset's ability to control a Critical Asset, but on whether the Cyber Asset performs monitoring or observation functions that could affect BES reliability.

BPA agrees with Recommendation 14. BPA has previously identified this area for improvement and developed a plan to create, document, and apply a combined Critical Cyber Asset identification methodology to assets in BPA's control centers and field locations.

BPA's new CCA identification methodology, developed as part of the plan mentioned in Recommendation 13, will focus on two key questions:
a. Do the Cyber Assets utilize qualifying connectivity?
b. Are the qualified Cyber Assets essential to the operation of the associated Critical Asset (or essential Element)?

The criteria used to determine essentiality will include communications path, automatic control, supervisory control, protection, restoration, voltage regulation, and inclusion in special protection systems and automatic generation control.

The identification of CCAs using the new methodology is expected to be complete by December 1, 2013.

Recommendation 15: Train employees on procedures describing the new field asset CCA identification process.

BPA agrees with Recommendation 15. BPA has previously identified this area for improvement and developed a plan to create, document, and apply a combined Critical Cyber Asset identification methodology to assets in BPA's control centers and field locations.

Personnel involved in the identification of CCAs in field locations will be trained by December 1, 2013 on the new procedures as part of the plan mentioned in Recommendation 13.

Recommendation 16: Communicate the new field asset CCA procedures and policies to all affected employees.

BPA agrees with Recommendation 16. BPA has previously identified this area for improvement and developed a plan to create, document, and apply a combined Critical Cyber Asset identification methodology to assets in BPA's control centers and field locations.

BPA will communicate the new field CCA identification procedures and policies to all affected employees by December 1, 2013.

BPA appreciates the opportunity to comment on the draft report.

Sincerely,

\S\ John L. Hairston

John L. Hairston, Chief Compliance Officer
Bonneville Power Administration
PO Box 3621
Portland, OR 97208

Cc: Ronald Oechsler, Federal Energy Regulatory Commission

Document Content(s)