



OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-18-47

September 2018

SOUTHWESTERN POWER ADMINISTRATION'S ASSET PROTECTION



Department of Energy
Washington, DC 20585

September 10, 2018

MEMORANDUM FOR THE ADMINISTRATOR, SOUTHWESTERN POWER
ADMINISTRATION

Michelle Anderson

FROM: Michelle Anderson
Deputy Inspector General
for Audits and Inspections
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on “Southwestern Power
Administration’s Asset Protection”

BACKGROUND

The Department of Energy’s Southwestern Power Administration (Southwestern) markets and delivers power produced from Federal water projects at wholesale rates. Southwestern operates and maintains 1,380 miles of transmission lines used to transmit power generated to 6 states, including Arkansas, Kansas, Louisiana, Missouri, Oklahoma, and Texas. In addition, Southwestern maintains infrastructure that includes electrical substations, transmission lines, towers, and power system control centers, which ultimately supplies electricity to about nine million end users. Southwestern is subject to requirements established by the Department and the North American Electric Reliability Corporation (NERC) to protect its mission critical and related bulk electric system assets¹ by conducting risk assessments of its most significant assets.

In 2003, the Office of Inspector General report on *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003) noted that Southwestern had not performed required risk assessments for its critical assets. In 2010, another Office of Inspector General report on *Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations—Follow-Up Audit* (DOE/IG-0842, October 2010) found that Southwestern had not updated required critical asset vulnerability and risk assessments. Since 2010, Southwestern has had nine security incidents at its bulk electric system assets that have caused approximately \$100,000 in copper and equipment theft and related damage to Federal property. These incidents included limited unauthorized entry to switch yards, with no access gained into any buildings with power system control equipment or personnel, and with no impact to the bulk electric system. Additionally, there was an instance of an unauthorized vehicle gaining access to the Primary Control Center’s parking lot by piggybacking off another vehicle through the main

¹ Bulk electric system assets encompasses all elements and facilities necessary for the reliable operation and planning of the interconnected bulk power system.

external gate for an unknown purpose. Given the significance of this subject matter, we initiated this audit to determine whether Southwestern was properly protecting its mission critical and related bulk electric system assets.

RESULTS OF AUDIT

We found that Southwestern had not always taken sufficient measures available to ensure that its mission critical and related bulk electric system assets were properly protected. Specifically, we found that:

- Southwestern had not always conducted and updated required comprehensive risk assessments at its mission critical and bulk electric system assets in accordance with Departmental requirements and as it had committed to do in response to a 2010 Office of Inspector General report recommendation; and
- Several physical security issues existed at the bulk electric system substation sites we visited during our audit.

Additionally, we noted that the lack of updated comprehensive risk assessments had persisted since we first reported the issue in October 2010.

These issues occurred and persisted because Southwestern had not made physical security at its asset sites an adequate level of priority. The security function at Southwestern had not been fully staffed for several years, and therefore, all elements of its security function fell upon one individual, the Security Officer. Additionally, various site inspections were not being conducted with the rigor necessary to ensure that security measures were in place and working effectively. By not making physical security an adequate priority, Southwestern cannot ensure that its assets are adequately protected.

In response to the prior Office of Inspector General reports, Southwestern had made a few enhancements in an effort to address the issues identified. For example, even though not fully documented, Southwestern had conducted impact level assessments for each of its bulk electric system assets' locations that were used to assign medium and low-impact sites based on NERC requirements.

Risk Assessments

Southwestern had not always conducted and updated required comprehensive risk assessments at its mission critical and related bulk electric system assets as required by Department policies and as agreed upon in response to the Office of Inspector General's previous 2010 audit recommendation. Mission critical assets, as defined by Department Order 470.3C – *(U) Design Basis Threat*, are assets essential to meeting Southwestern's assigned mission. This designation is based on the impact of loss or disruption to Departmental missions and the determination that these facilities warrant an elevation of security beyond that specified in Departmental directives for general Government property or facilities. Southwestern identified two mission critical assets, the Primary Control Center and the Alternate Control Center, for which risk assessments

are required to be conducted by Department Order 470.3C. However, we found that Southwestern had not conducted a risk assessment at its Alternate Control Center, as required by Department policy. These assessments include evaluating existing security systems, analyzing current threat information, identifying and implementing security measures needed to reduce risk, and documenting the level of risk that management is willing to accept on individual mission critical assets. Southwestern officials indicated that they had not performed a risk assessment at the Alternate Control Center, which is located at a U.S. Army Corps of Engineers facility, and serves as the backup to Southwestern's Primary Control Center. Officials stated their belief that the protection measures in place were more than sufficient. Officials added that even though an official risk assessment had not been documented, security was constantly being assessed as part of Southwestern's NERC compliance efforts and coordination with the owner of the site where the Alternate Control Center is located. While we agree that there were multiple layers of security protecting the Alternate Control Center, it is required that Southwestern conduct and maintain up-to-date risk assessments that evaluate the existing security system, analyze current threat information, and identify security enhancements needed to reduce risks. Without performing an adequate risk assessment, Southwestern cannot ensure that it has taken the necessary steps to deter, prevent, and mitigate all security risks and threats for this mission critical asset.

Further, while Southwestern had formal risk assessments for the Primary Control Center and its bulk electric system assets (including substations and switching stations) as required by Department Order 470.3C, we found that the risk assessments had not been effectively updated since fiscal year 2004. Specifically, in response to our 2003 audit report, *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003), initial risk assessments were conducted by Southwestern to address our finding that it had not adequately assessed the vulnerabilities and risks for its critical assets. Southwestern also conducted risk assessments in fiscal year 2004 for its bulk electric system assets.

In response to a recommendation in our 2010 report, Southwestern committed to update risk assessments at least once every 5 years. However, while Southwestern indicated that it had prepared assessments in 2011 and 2015, we found that these assessments were not updated and/or revised.

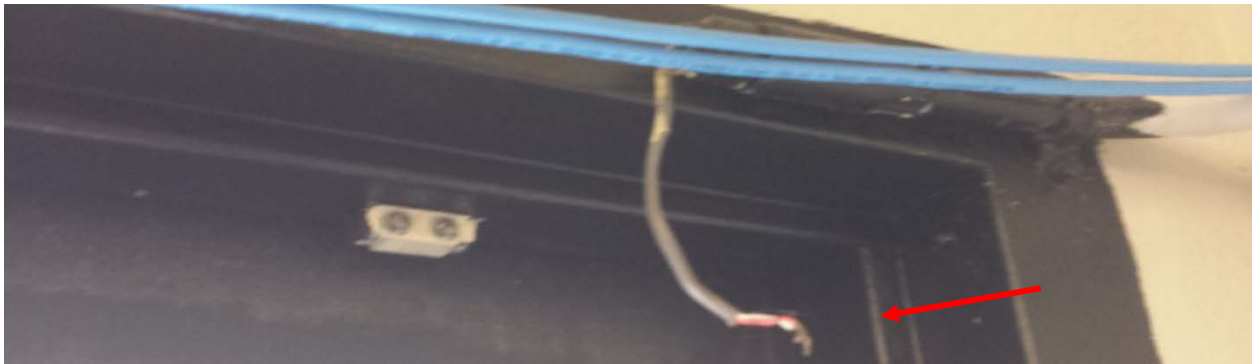
Our review found that the original recommendations from the initial assessments performed by Southwestern in 2004 had not been revised or updated to capture disposition activities in its subsequent assessments. For example, 2004 assessments performed by Southwestern at its switching stations and substations indicated that control building doors were alarmed, but these alarms were of low quality and not monitored. Subsequent to its 2004 assessment, Southwestern took action on the risk assessment recommendations and ensured that door alarm contacts were installed and began monitoring the doors. However, this update to the door alarms, and possibly other changes, had not been captured or acknowledged in the 2011 and 2015 revised versions of the assessments. Additionally, the analyses worksheets and images included in the assessments were dated in the 2003 and 2004 timeframe, with no updates. Further, we noted that the last page of each assessment was a change tracking chart, which stated that Southwestern performed a review of the document and found no change in site conditions, potential threats, or risks. The updated or revised assessments should have addressed any new potential threats or changes in

the physical security systems. Without performing an adequate update to the risk assessments and consideration of any new threats or vulnerabilities, Southwestern has not put itself in the appropriate position to protect its assets.

Additionally, during our site visit, we found a vulnerability that had been reported in a 2004 assessment performed by Southwestern that remained uncorrected and was still a vulnerability almost 13 years later. Specifically, during the assessment process, Southwestern conducted site surveys for each of its assets to look at potential vulnerabilities and likely attack scenarios. In the site survey for one of its switching stations, Southwestern found that the door alarm contact for the side door to the control building had been disconnected. The assessment included a specific recommendation to repair/rewire the door alarm contact. During our walk-through of the switching station in July 2017, we found that the previously identified door alarm contact remained disconnected. See the 2004 and 2017 images of the disconnected door contact below:



Switching Station Door Alarm Contact – 2004 Assessment Image



Switching Station Door Alarm Contact – July 2017 Site Walk-Through

As illustrated in the pictures above, the door had since been painted; however, the alarm contact remained disconnected. Subsequent to our review, we were informed that Southwestern officials had taken corrective actions and had the door alarm reconnected. Additionally, Southwestern officials indicated that as of March 2018, the Division of Maintenance had instructed its employees to test all door alarms at the control buildings during the bi-monthly inspections.

Physical Security Issues

During our physical walk-throughs of Southwestern's assets, we identified a number of physical security issues, such as significantly overgrown vegetation within a substation, trees hanging

over and on fences, poorly installed barbed wire topper, poor fence repairs, fence dig outs and/or wash outs, and bushes growing through fences. Southwestern's Site Security Plan required that all assets be configured to protect Government-owned property and equipment against damage, destruction, or theft and to provide a means to control public access. For example, assets are secured with fences to deter and delay unauthorized access and excess vegetation is eliminated to reduce the risk of fires. While we understand that it is not economically feasible to fully protect the assets from all potential issues, increasing the safety and security capabilities through improved detection, delay², and assessment in any way possible can reduce risk exposure. Regular maintenance and inspection of assets should identify and remedy these types of issues in a timely manner. See the following images for examples of the issues noted during our site walk-throughs:



Trees hanging over fences at a switching station could potentially damage the fence, allow someone to climb the tree and gain access, and pose a fire hazard.

² Delay is the second required function of a security system, as it helps impede an adversary's progress into a protected area. Delay can be accomplished by fixed or active barriers, (e.g., fences, doors, vaults, locks) or by sensor activated barriers (e.g., dispensed liquids, foams).



Overgrown vegetation poses potential fire hazard and limits visibility at a substation.



Poor fence repair at the site of a previous break-in compromises security at a tap station and makes it easier to gain access to the asset.



A gap under the fence at a tap station could allow access by a person or animals.



Bushes growing through a fence at a substation create a fire hazard, provide cover to potential intruders, and impair the vision of anyone monitoring the substation.

Additionally, we found that Southwestern's Key Control Inventory Log had not been kept up-to-date in accordance with its Site Security Plan. During our site visits, a Southwestern employee escorted us to each asset and unlocked all the gates and control houses with his assigned keys. However, subsequent to our trip, we found that he was not listed on any of the Key Control Inventory Logs as having keys for the gates or control houses for which he granted us access. Loss of control over the inventory of keys increases the potential that unauthorized users or an insider threat could gain access to Southwestern assets. Subsequent to our site visit, Southwestern officials have updated the Key Control Inventory Log to include this individual's keys.

Priority of Physical Security at the Assets

These issues occurred because Southwestern had not made physical security at its asset sites an adequate level of priority. Specifically, Southwestern had not fully staffed its security function, and therefore, all elements of its security fell upon one individual, the Security Officer. At the time of our walk-throughs of 17 Southwestern substations and control center facilities, the Security Officer, who has been in place since 2014, acknowledged that he had never been to a number of the sites. Also, he was not always aware of what security measures were in place at the sites. Additionally, the Security Officer indicated that as the only individual handling routine security tasks, a significant portion of his time was spent on activities such as on-boarding new hires, background checks, and badging issues. He stated that handling these routine tasks left inadequate time for additional security activities such as risk assessments and site security inspections.

Further, various site inspections had not been conducted with the rigor necessary to ensure that security measures were in place and working effectively. For example, Southwestern's maintenance division conducted bi-monthly inspections of the substations and was tasked with ensuring that actions were taken to correct any noted deficiencies. These inspections examined fences, gates, locks, yard lights, and yard appearance; control room door alarms; and housekeeping. For at least the last two and a half years, the inspection reports at one switching station indicated that the doors and alarms were tested and operational; however, as noted above, we found that the side door alarm was disconnected. This was an unmanned remote facility that relied on these alarms to ensure that the site was protected against potential thieves, vandals, and saboteurs from destroying/damaging equipment and accessing the transmission network. However, with the door alarm disconnected, there was no monitoring in place on the side door to ensure that the control room was secure. While Southwestern maintained multiple internal tracking systems to manage its maintenance and information technology groups' work order flows, there was not a formal mechanism in place, such as formal corrective action plans and necessary followup, for Security to ensure that required physical security measures identified in risk assessments and site inspections had been addressed.

Additionally, Southwestern officials informed us that the lack of key inventory control had been due to inadequate recordkeeping practices. As such, since our site visit, the Security Officer's keys have been added to the Key Control Inventory Logs.

Assurance that Assets are Adequately Protected

One of the Department's key priorities is its role in ensuring the reliable supply and delivery of energy. By not making physical security an adequate level of priority, Southwestern's capability to adequately protect its assets is diminished. This lack of adequate prioritization increases the risk of trespassing, vandalism, destruction, and sabotage at Southwestern's high-dollar value bulk electric system assets. In light of the weaknesses identified, we made several recommendations that, if fully implemented, should help improve Southwestern's security over mission critical and related bulk electric system assets.

RECOMMENDATIONS

To address the issues identified in our report, we recommend that the Administrator for Southwestern Power Administration:

1. Review and analyze Southwestern's Security Office staffing level to ensure that it is commensurate with expected workload so that all necessary security initiatives and requirements, such as conducting and updating comprehensive risk assessments for mission critical and related bulk electric system assets, can be accomplished in a timely manner;
2. Ensure that bi-monthly substation inspections are conducted thoroughly and consistently and that identified physical security issues, including those noted in this report, are addressed in a timely manner;
3. Ensure that all access keys to substation gates and control houses are accounted for and maintained by authorized personnel; and
4. Develop corrective action plans and a tracking system to ensure physical security issues identified in risk assessments and site inspections are addressed in a timely manner.

MANAGEMENT RESPONSE

Management concurred with our report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Specifically, management stated that a vacancy announcement had recently been published for a Security Specialist to allow for more timely completion of physical security assessments and greater capacity for making physical security system improvements. Additionally, clarifying direction has been issued for facility inspections and maintenance, including an annual maintenance and testing program for physical security alarms and systems, and a database for maintenance and repair issues. Further, Southwestern committed to implementing an access control system on all control houses and procuring or developing a key management software for tracking keys. Finally, Southwestern plans to install software to track maintenance/improvement tasks for access control, surveillance, and physical barrier systems. Management comments are included in Attachment 3.

AUDITOR COMMENTS

We consider management's comments and proposed corrective actions to be responsive to our recommendations. We recognize that management has already taken some actions to improve processes and physical security issues in response to our audit work.

Attachments

cc: Deputy Secretary
Chief of Staff
Under Secretary of Energy

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

We conducted this audit to determine whether the Southwestern Power Administration (Southwestern) was properly protecting its mission critical and related bulk electric system assets¹.

SCOPE

The audit was performed between June 2017 and September 2018 at Southwestern's Headquarters office in Tulsa, Oklahoma. Walk-throughs were conducted at 17 Southwestern assets located in Oklahoma, Missouri, and Arkansas. The audit was conducted under Office of Inspector General project number A17PT030.

METHODOLOGY

To accomplish our audit objective, we:

- Reviewed laws, regulations, and other guidance applicable to the security and protection of mission critical and related bulk electric system assets;
- Interviewed Southwestern officials responsible for the security of mission critical and related bulk electric system assets;
- Reviewed Southwestern's Site Security Plan and Design Basis Threat Implementation Plan;
- Interviewed Southwestern officials to determine if performance measures related to the protection of Southwestern's assets existed;
- Reviewed security incident reports and related documents for Southwestern's assets;
- Conducted walk-throughs at 17 judgmentally sampled assets to observe the physical security measures in place. The sample was selected to include both control centers, as well as additional substations and switching stations within two of the three Southwestern regions. Because a judgmental sample was used, the results were limited to the assets selected; and
- Analyzed initial and revised risk assessments for Southwestern's mission critical and related bulk electric system assets, when available.

¹ Bulk electric system assets encompasses all elements and facilities necessary for the reliable operation and planning of the interconnected bulk power system.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Accordingly, the audit included tests of controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed compliance with the *GPRA Modernization Act of 2010* and determined that Southwestern had not established performance measures related to security at the mission critical and related bulk electric system assets. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not rely on computer-processed data to satisfy our audit objective, and therefore, did not conduct a reliability assessment of computer-processed data.

An exit conference was held with management officials on September 6, 2018.

PRIOR REPORTS

- Audit Report on [*Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations – Follow-up Audit*](#) (DOE-IG-0842, October 2010). The review found that many Power Marketing Administration efforts essential to identifying current risks or threats and mitigating those risks remained incomplete. While a number of activities relevant to critical infrastructure protection had been initiated, the Power Marketing Administrations had not: (1) completed and updated, when appropriate, all required vulnerability and risk assessments; and (2) conducted required tests to ensure that security measures for physical assets were operating as designed. Further, Bonneville Power Administration and Western Area Power Administration had not implemented security enhancements recommended in completed risk assessments.
- Audit Report on [*Power Marketing Administration Infrastructure Protection*](#) (OAS-B-03-01, April 2003). The review found that while Bonneville Power Administration had performed adequate vulnerability and risk assessments for its most critical assets, assessments were either inadequate or did not exist at Western Area Power Administration and Southwestern Power Administration. This occurred at Western Area Power Administration because it had emphasized emergency recovery rather than assessing all of its assets' vulnerabilities and risks. At Southwestern Power Administration, management stated that its security team's workload and travel restrictions limited the priority placed on completing the assessments. As a result, these two Power Marketing Administrations' assets could be more vulnerable to attack. Moreover, the consequences of an attack could be more severe than necessary, including: (1) impacts on employees and assets; (2) a decrease in mission capabilities; and (3) economic impacts on the Power Marketing Administrations and their customers.

MANAGEMENT COMMENTS




Department of Energy
 Southwestern Power Administration
 One West Third Street
 Tulsa, Oklahoma 74103-3502

OFFICE OF THE ADMINISTRATOR

DATE: August 28, 2018

MEMORANDUM TO: Sarah B. Nelson
 Assistant Inspector General
 for Audits and Administration
 Office of Inspector General

FROM: Mike Wech 
 Administrator
 Southwestern Power Administration

SUBJECT: Draft Audit Report on "Southwestern Power Administration's
 Asset Protection", IG-302 (A17PT030)

Thank you for the opportunity to comment on the subject draft report. Southwestern appreciates the efforts the Office of Inspector General has made to identify areas for improvement in Southwestern's asset protection program. Below are responses to each recommendation found in the draft report. Additional technical comments are found in the attachment.

Recommendation #1: Review and analyze Southwestern's Security Office staffing level to ensure that it is commensurate with expected workload so that all necessary security initiatives and requirements, such as conducting and updating comprehensive risk assessments for mission critical and related bulk electric system assets, can be accomplished in a timely manner.

Management Response: Concur. A vacancy announcement for a Security Specialist at the Springfield, MO facility was published August 13, 2018. The addition of the Security Specialist will allow more timely completion of physical security assessments and greater capacity for making physical security system improvements.

Recommendation #2: Ensure that bi-monthly substation inspections are conducted thoroughly and consistently and that identified physical security issues, including those noted in this report, are addressed in a timely manner.

Management Response: Concur. Southwestern's Director of Maintenance issued direction to staff March 29, 2018, instructing that each alarmed door be checked individually and that each alarm test result be verified with Operations Dispatch during the bi-monthly inspections. The Southwestern Administrator recently issued a memo to the Director of Maintenance providing

further clarity on the processes to be used to increase effectiveness of facility inspections and maintenance. Southwestern will implement an annual maintenance and testing program for physical security alarms and systems, which will include a database for maintenance and repair issues. The target date for the implementation of this system is January 31, 2019.

Recommendation #3: Ensure that all keys to substation gates and control houses are accounted for and maintained by authorized personnel.

Management Response: Concur. Southwestern is implementing an access control system on all control houses, which will reduce the number of keys issued. The access control system will provide a “point zero” when current keys no longer provide access, negating the threat of possible unaccounted for keys. This system will include keys which are “copy resistant” and individually numbered. Contracted installation is planned for completion by December 2019. Southwestern’s gates will also be rekeyed, invalidating possible unaccounted for keys, and a copy resistant key similar to those proposed for substation control houses will be used. Completion for all substation gates is planned to be completed by June 2019. Southwestern will procure or develop a key management software that will properly track the issuance of keys to personnel, and what access each key grants. The target date for completion of the acquisition of development of the key management system is April 2019.

Recommendation #4: Develop corrective action plans and a tracking system to ensure physical security issues identified in risk assessments and site inspections are addressed in a timely manner.

Management Response: Concur. Southwestern’s current effort to establish a maintenance and testing program includes procurement or development of software to track maintenance/improvement tasks for access control, surveillance and physical barrier systems. The target date to fully implement the software is December 31, 2019.

If you have any questions regarding this response, please contact Ms. Missy Valencia, Audit Coordinator, (918) 595-6719, Missy.Valencia@swpa.gov.

attachment

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions, and feedback to OIG.Reports@hq.doe.gov and include your name, contact information, and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.