U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

Followup on Western Area Power Administration's Critical Asset Protection

DOE-OIG-16-11

April 2016

Department of Energy
Washington, DC 20585

April 4, 2016

MEMORANDUM FOR THE SECRETARY

FROM: Rickey R. Hass
Acting Inspector General

SUBJECT: INFORMATION: Audit Report on the "Followup on Western Area Power Administration's Critical Asset Protection"

BACKGROUND

The Department of Energy's Western Area Power Administration (herein referred to as Western and WAPA) markets and transmits electrical power across 15 states to wholesale customers. It maintains an extensive infrastructure, including electrical substations, high-voltage transmission lines and towers, and power system control centers. Western is subject to security requirements established by the Department, the North American Electric Reliability Corporation (NERC), and the Department of Homeland Security. As of November 2014, Western officials identified a number of electric substations and power system control centers as critical assets based on existing and draft NERC requirements. Critical assets are those facilities, systems, and equipment that, if rendered inoperable or damaged, would affect the reliability or operability of the electric system. Western protects its critical assets by conducting risk assessments of security systems; analyzing threat information; identifying and implementing physical security measures to reduce risk; and documenting the level of risk that management is willing to accept for each asset.

In 2003, the Office of Inspector General audit report on *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003) noted that Western's risk assessments were inadequate. In 2010, our report on *Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations—Follow-up Audit* (DOE/IG-0842, October 2010) found that Western had not completed required risk assessments and security measure performance testing, and had not implemented physical security enhancements recommended in completed risk assessments. We initiated this followup audit to determine whether Western had effectively and efficiently managed the protection of its critical assets.

RESULTS OF AUDIT

Although Western had initiated efforts to improve physical security and protection of its critical assets, we found that significant issues still existed and issues identified in our 2010 report remain unaddressed. Specifically, we found that Western had not always:

- Established adequate physical security measures and practices for its critical assets;
- Addressed physical security measures recommended in prior risk assessments; and
- Conducted performance testing to ensure that security measures for physical assets were performing as designed.

Specific examples of physical security measures and practices that were not sufficient included instances in which regions had not implemented all of Western's minimum security requirements for critical assets as outlined in WAPA Order 470.1H, *Safeguards and Security Program*; repaired or replaced malfunctioning, inoperable, or degraded security equipment; or established adequate controls over issuing keys to access critical substation gates and control buildings.

The issues we identified occurred in large part because Western had not placed sufficient emphasis on physical security. We also found that Western lacked specific policies and procedures for maintaining security equipment, controlling access keys, implementing risk assessment recommendations, and conducting performance tests.

While much remains to be done, Western had taken a number of positive actions to improve the physical security of its critical assets. Specifically, in fiscal year (FY) 2013, Western established the Office of Security and Emergency Management (OSEM), and in FY 2014, Western centralized within OSEM the security programs that had separately existed at each of Western's four regions: Rocky Mountain, Sierra Nevada, Upper Great Plains, and Desert Southwest. Among other responsibilities, OSEM was tasked with conducting risk assessments and identifying necessary physical security measures, and by December 2014, OSEM had conducted assessments on all of Western's critical assets. However, we noted that while OSEM had program authority, it did not have authority to fund and implement recommended measures. According to Western officials, each region remains responsible for implementing, prioritizing, and funding physical security measures recommended in the risk assessments due to fund sources and repayment issues.

A Western official informed us that, based on the 2014 assessments, OSEM intends to assist the regions with developing corrective action plans and establishing timelines to implement recommended physical security measures. However, one official expressed concern that the regions may not fund and implement the recommended physical security measures, based on how little the regions had spent on physical security in the past.

Protecting critical infrastructure[1] is essential to the Nation's security and economic vitality. As noted in the Department's April 2015 *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, physical attacks on critical infrastructure are a growing concern and, while some physical security measures are in place, additional low-cost investments at sensitive facilities would greatly enhance resilience. The consequence of tampering with or

[1] Per the National Infrastructure Protection Plan, critical infrastructure represents systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

destroying equipment in substation yards and control buildings could cause significant disruption in the functioning of Government and business, potentially producing a cascading effect far beyond the physical location of the incident.

These concerns are not merely theoretical. Western had experienced instances where its critical assets had been penetrated and, in some cases, Western did not have the physical security capabilities to promptly detect the intrusions. One of the intrusions resulted in damage to the perimeter fence and control building door, and the theft of a security camera and tools. Although not a Western-owned asset, the impact of malicious activity is well demonstrated by a 2013 physical attack on the substation of a utility located in California, which resulted in $15.4 million in damages to 17 transformers and 6 circuit breakers. Because of these recent events and the importance of securing the bulk electric system, we made recommendations designed to improve Western's physical security and to reduce the risk of damage to its critical assets.

Due to the sensitive nature of the vulnerabilities identified during our audit, specific region locations have been omitted from this report. We separately communicated to Western officials the specific regions and critical assets affected.

MANAGEMENT RESPONSE

Western concurred with the recommendations and indicated that corrective actions were planned to address the identified issues. Western indicated that it is committed to continually improving its security posture and will implement the recommendations to enhance its Physical Security and Assessment Program. We considered Western's response and planned actions to be responsive to our recommendations. Western's formal comments are included in Appendix 3.

Attachments

cc: Deputy Secretary
Chief of Staff
Administrator, Western Area Power Administration

FOLLOWUP ON WESTERN AREA POWER ADMINISTRATION'S CRITICAL ASSET PROTECTION

TABLE OF CONTENTS

Audit Report

Details of Finding 1

Recommendations 9

Management Response and Auditor Comments 10

Appendices

1. Objective, Scope, and Methodology 11
2. Prior Reports 13
3. Management Comments 14

DETAILS OF FINDING

In 2014, the Department of Energy's Western Area Power Administration (herein referred to as Western and WAPA) reported that it served approximately 680 wholesale power customers and managed more than 328 substations, 177,000 structures, and 26 facilities, covering a footprint of more than 1.3 million square miles and making it 1 of the 10 largest transmission providers in the United States. Western's greatest responsibility and the root of its mission is to manage its infrastructure, valued at nearly $4 billion.

To strengthen and maintain a secure, functioning, and resilient national critical infrastructure, the President issued President Policy Directive-21, *Critical Infrastructure Security and Resilience,* in February 2013. The directive applied to all critical infrastructures but calls out energy infrastructure as being "uniquely critical" due to the enabling functions they provide across all of the critical infrastructures. Given the significance of Western's infrastructure to the energy sector, it is of the utmost importance to protect its critical assets from potential maleficent occurrences, such as unauthorized access, theft, vandalism, attack, and sabotage. As of November 2014, Western officials identified a number of electric substations and power system control centers as critical assets based on North American Electric Reliability Corporation (NERC) requirements. Critical assets are those facilities, systems, and equipment that, if rendered inoperable or damaged, would affect the reliability or operability of the electric system.

In fiscal year (FY) 2013, Western established the Office of Security and Emergency Management (OSEM), and in FY 2014, Western centralized within OSEM, the security programs at each of Western's four regions: Rocky Mountain, Sierra Nevada, Upper Great Plains, and Desert Southwest. Among other responsibilities, OSEM is currently tasked with conducting risk assessments that include threat and vulnerability assessment strategies and identifying necessary measures needed to protect Western's critical assets. Each region, according to a Western official, remains responsible for the implementation, prioritization, and funding of physical security measures recommended in the risk assessments.

Although Western had initiated efforts to improve physical security and protection of its critical assets, we found that significant issues still existed and issues identified in our 2010 report on *Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations–Follow-up Audit* remain unaddressed. Specifically, we found that Western had not always:

- Established adequate physical security measures and practices for its critical assets;
- Addressed physical security measures recommended in prior risk assessments; and
- Conducted performance testing to ensure that security measures for physical assets were performing as designed.

Physical Security Measures and Practices

We found that Western had not always established adequate physical security measures and practices for its critical assets. For example, we found instances in which Western had not implemented all required minimum security requirements at its critical assets; repaired or replaced malfunctioning, inoperable, or degraded security equipment; and established adequate controls over issuing keys to access critical substation gates and control buildings.

Minimum Security Requirements

During our visits to six critical assets in two regions, we observed that minimum security standards required in WAPA Order 470.1H, *Safeguards and Security Program*, were not always met. Minimum security standards, as part of an overall physical security policy, provide for protection of personnel and assets. At the six critical assets visited, we found the following noncompliance with minimum standards:

- Lack of barbed wire at the top of the perimeter fence to prevent unauthorized entry;
- A perimeter access gate left unlocked and unattended;
- Lack of audible alarms that would annunciate within 10 seconds of the substation control house or power system control center door not properly closing;
- Lack of lighting that could be controlled remotely from the power system control centers; and
- Landscaping that could permit the concealment of dangerous objects or obstruct the view of the perimeter by security personnel and cameras.

Moreover, in our review of prior risk assessments at other regions, we noted that one region’s power system control center did not have a perimeter fence, even though it was a minimum security requirement and identified as a finding in a February 2011 risk assessment. The regional manager authorized an exemption for the implementation of the perimeter fence, asserting that a fence would draw unneeded attention to an already obscure building and that the building currently had force protection measures in place, including fortified exterior and interior walls; perimeter cameras; and landscaping berms. Although WAPA Order 470.1H allows exemptions to minimum standards if they are documented and approved by the regional manager, it does not specify acceptable conditions for such exemptions. Given that power system control centers are one of the more essential components of the transmission system because they continuously operate and monitor the transmission grid, we find it concerning that the regional manager had approved an exemption from implementing a minimum security requirement for the region’s power system control center. Despite the regional manager’s decision, the September 2014 risk assessment still recommended a perimeter fence. Western officials informed us that as of October 2015, they had developed a draft approach to make the exemption process a more formal, documented process in which exemptions would be based on threat factor analyses.

Repair and Replacement of Security Equipment

Department Order 473.3, *Protection Program Operations*, required security related subsystems and components to be maintained in operable condition. Despite this requirement, Western had not always repaired or replaced malfunctioning, inoperable, or degraded security equipment. For example, at one region, malfunctioning equipment that had not been repaired contributed to a slow response during a November 2013 incident in which a critical substation's control building was penetrated, and the breach remained undetected for more than 2 days. The incident review report noted that there were known issues with the contact alarms on the doors of the control building that had not been resolved, and a decision was made for dispatch to ignore alarms due to the number of false alarms. According to a regional official, the contact alarms on the doors had been malfunctioning for almost a year, and video surveillance trailers used to monitor the yard and the substation's perimeter were also not working. Furthermore, it was reported in a September 2014 Physical Security and Risk Assessment for another of the region's critical substations that one of the cameras that provided a view of an access road had not been operational for over a year.

A regional official also informed us that cameras installed at three critical assets were approximately 12 years old and in need of replacement. Officials informed us that although these cameras were operational, they tended to freeze and require rebooting and the quality of the video feed varied. In addition, this official told us many sites needed a complete overhaul of their security systems and most cameras at the substations had limited coverage of the yard and no nighttime capability. We noted that the 2014 risk assessments for two of the three critical assets visited during our audit corroborated some of the official's assertions about the region's camera system limitations. Moreover, the official also stated that the security systems in place had been installed piecemeal, encompassing many different systems that did not have detection capabilities, making it difficult for security personnel to properly monitor the critical assets. During our site visit, we observed that security personnel had to actively watch a large monitor that displayed feeds from approximately 89 cameras because the majority of the monitoring systems did not have the capability to trigger an alert when motion was detected. In addition, the incident report for the previously discussed November 2013 breach, identified the lack of a single video monitoring system and an intrusion detection system as contributing factors for the breach going undetected for more than 2 days.

Access Key Controls

The two regions we visited did not adequately safeguard the distribution of access keys to perimeter gates or control buildings at their substations. WAPA Order 470.1H requires establishing a key control accountability program to ensure that keys are controlled and distributed in a systematic manner. One region provided remote controls and padlock keys to employees for accessing automated and mechanical perimeter gates. We found that logs documenting which employee had remote controls or keys were not maintained. The log for remote controls was not updated when employees departed employment or when new employees commenced work. For mechanical gates, although a regional official provided us with a key log, the official told us that he could not verify that all the keys were represented on the list. The log was created after the keys had been in circulation for several years and, therefore, there was no history of the number of keys purchased or any knowledge of the keys taken out of circulation.

At the other region, we also found weak controls over access keys to perimeter gates and card keys to unlock control buildings. Specifically, we found that there was no mechanism to account for and track the distribution of perimeter gate keys, such as a log or spreadsheet. Although the region had a process in place to ensure employees had authorization prior to distributing keys to perimeter gates, there was no accountability for the keys after distribution.

Risk Assessment Recommendations

We found that Western had not always addressed recommended physical security measures identified in risk assessments, a recurring issue that we had previously reported in 2010. Based on our review of 37 Facility Security Assessments conducted between FY 2010 and FY 2013 throughout all of Western's regions, we noted that six of the nine recommendations considered mandatory to mitigate high-risk threats had not been implemented as of January 2015. For example, an April 2011 risk assessment had a mandatory recommendation to install additional cameras within the perimeter of the substation and, as of December 2014, regional officials responded that a camera evaluation was still in progress. Furthermore, in only one of these six cases had the regional manager approved an exemption, and thereby accepted the risk of not addressing a mandatory physical security measure.

In addition, Western did not address 25 of the 62 recommended physical security measures that were considered optional. Western's risk assessments defined optional recommendations as those that address moderate or low threats, or instances in which there was no nationally recognized minimum standard requirement. While we understand that these recommended physical security measures were considered optional, we found no decision documents justifying why some optional recommendations were implemented, while others were not. For example, no justification was provided by the region for not addressing an optional recommendation identified in a September 2011 risk assessment to install razor wiring on the top of a substation's perimeter fence to deter unauthorized access.

In addition, we found that perimeter intrusion detection systems, although recommended since 2002, had not been installed at five of Western's critical assets. In our 2010 audit report, we noted that Western had not installed electronic perimeter intrusion detection systems recommended in its 2002 and 2008 risk assessments at 17 critical assets, and lacked the documentation needed to justify decisions to forego recommended measures and accept the additional risk. We found that as of November 2014, 15 of those assets were still identified as critical and perimeter intrusion detection systems remained uninstalled at 5 critical assets. Furthermore, intrusion detection systems were still being recommended for installation in the 2014 risk assessments for all five critical assets.

WAPA Order 470.1H required that Western document all assessments and related recommendations in its asset management system and generate and forward the appropriate work orders required to correct any security deficiencies to the appropriate maintenance staff.

However, we found that none of the regions had followed this requirement or created corrective action plans to ensure recommended physical security measures were implemented. Western officials informed us that risk assessments were conducted at one point in time. Although they recognized that findings from past assessments had not always been addressed, the current posture of those critical assets (including demographics, site specific threats, and mission) could have changed; therefore, they would not retroactively implement recommendations from prior assessments. Rather, upon finalization of the risk assessments conducted in 2014, they intend to assist the regions with developing corrective action plans and establishing timelines to implement recommended physical security measures. They also told us that they are in the process of modifying Western's policy to require that both the regional manager and Western's Administrator sign a risk acceptance form that justifies the risk for not remediating an identified deficiency and assumes responsibility for that decision. Finally, the Chief Operating Officer told us that he intends to make all compliance-related recommendations from the 2014 assessments a priority.

Performance Testing

Western had not always conducted performance testing to ensure that physical security measures were performing as designed, in accordance with Department Order 470.4B, *Safeguards and Security Program*; Department Order 473.3; WAPA Order 470.1H; and *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*. According to Department Order 470.4B, a performance assurance program must be developed that identifies the essential elements of a protection program and establishes monitoring and testing activities with sufficient rigor to ensure that the program elements are at all times operational, functioning as intended, and interacting in such a way as to identify and preclude occurrence of adverse activity before security is irreversibly compromised. Testing encompasses such elements as determining whether equipment is calibrated properly, security guards are knowledgeable in procedures, and intrusion detection systems are activating properly.

Only one of Western's regions conducted testing on all of the security components (such as door alarms and access card readers) at its critical assets to ensure the equipment functioned as intended. The other three regions had conducted testing to meet NERC Critical Infrastructure Protection standards; however, we found that such testing was not always performed at all of Western's non-cyber critical assets or on all security equipment, such as cameras, video analytics, and door contacts. In addition, we found that none of Western's regions implemented tests to ensure overall system effectiveness. The failure to conduct tests of overall system effectiveness was also identified as a longstanding issue in our 2010 report.

The lack of testing limits Western's ability to identify vulnerabilities and make improvements where necessary. To Western's credit, it intends to conduct performance testing in the future, and as of October 2015, Western officials informed us that they had acquired a contractor to develop a performance testing program.

Management of Western's Critical Asset Protection

The issues we identified occurred in large part because Western had not placed sufficient emphasis on physical security. Western's Chief Operating Officer told us that, prior to 2013, Western's safety and security functions were combined and that more emphasis had been placed on the safety function because the personnel hired possessed safety expertise and were not as knowledgeable on security requirements. Similarly, we noted that regional officials were unaware of all required minimum security standards, and one regional official informed us that many individuals in his region were not aware of WAPA Order 470.1H. To their credit, Western's Chief Operating Officer stated that after our last report in 2010, he realized that the lack of expertise was an issue and began the process to separate security from safety and centralize the security function, which resulted in the establishment of OSEM in 2013.

In addition, we found that Western lacked specific policies and procedures related to security equipment maintenance, controls over access keys, implementation of risk assessment recommendations, and performance testing. Specifically:

- One region we visited lacked formal policies and procedures to report and track needed repairs and replace degraded or inoperable equipment. The region's process to address maintenance repairs was, for the most part, informal and reactive. Regional officials stated that when maintenance issues were identified by security personnel, an email would be sent to the maintenance officials responsible for repairing and maintaining the security equipment. However, the needed repair and related corrective actions were not logged in a central location to ensure repairs to security equipment were completed. As a result of our audit, a regional official informed us that backlogged security repairs were now being addressed more promptly by dedicating an employee to this effort; however, the overall issue with repairing or replacing malfunctioning, inoperable, or degraded security equipment remained. We also noted that the region lacked a security equipment replacement plan to ensure scheduled timeframes were established to replace or upgrade defective or aging security equipment.

- The two regions we visited also did not have specific policies and procedures to ensure that adequate key controls were in place. Although WAPA Order 470.1H stated that each office shall establish a key control accountability program, it did not provide specific guidance on the procedures that should be followed to ensure an adequate accountability program. Processes currently in place did not ensure that access to critical assets was adequately controlled because gate and door key listings were not updated and in some instances did not exist. Moreover, there was no process to ensure keys were returned upon the departure of an employee.

- WAPA Order 470.1H did not clearly specify parameters, procedures, or policies detailing circumstances under which security measures should be implemented and did not include a procedure for holding Western officials accountable for addressing recommended physical security measures. Even though Western's risk assessments defined "mandatory" and "optional" recommendations, WAPA Order 470.1H did not include this definition, and neither the risk assessment methodology nor the Order specified a process or a methodology to implement the "optional" recommendations. Furthermore, Western did not require corrective action plans or documented decisions and explanations as to why optional recommendations were or were not implemented.

- Western had not developed a performance assurance program, as required by Department Order 470.4B, to ensure that it had conducted performance testing as required. In addition, because of recent changes in some senior management and security personnel in the regional offices since our last audit, we were unable to identify specifics regarding why a performance assurance program was not implemented.

We observed a number of positive actions by OSEM to strengthen physical security at Western, including conducting risk assessments and drafting changes to Western's policies to ensure better accountability. In addition, OSEM plans to assist the regions on developing corrective action plans based on the results of the risk assessments conducted in 2014. However, we noted that although OSEM had program authority, it did not have authority to fund and implement recommended physical security measures. A Western official told us that such authority and funding decisions remain at the regions and expressed concern about the regions not funding and implementing recommended physical security measures in the 2014 risk assessments. The official also expressed the need for more resources and funding to ensure the protection of Western's critical assets and stated that he was surprised by how little the regions had spent on physical security in the past. Based on Western's history of not always implementing recommended physical security measures, as identified in this report and our prior report, we share this official's concern that the regions may continue not to prioritize, implement, and fund needed physical security measures.

In May 2015, the Chief Operating Officer stated that Western Headquarters, in collaboration with the regions, intends to integrate security funding into the regional asset management plans, which are 10-year plans outlining future funding to replace and maintain infrastructure. However, an official stated that in the past, money previously allocated to improve the security of one of Western's critical assets had been reallocated to repair other failing equipment.

Impact and Path Forward

Protecting critical infrastructure is essential to the Nation's security and economic vitality. As noted in the Department's April 2015 *Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure*, physical attacks on critical infrastructure are a growing concern and, while some physical security measures are in place, additional low-cost investments at sensitive facilities would greatly enhance resilience. The consequence of tampering with or destroying equipment in substation yards and control buildings could cause significant disruption in the functioning of Government and business, potentially producing a cascading effect far beyond the physical location of the incident.

These concerns are not merely theoretical. Western experienced instances where its critical assets had been penetrated, and intrusions were not detected by Western's physical security measures or its security personnel in a timely manner. Most alarming was the November 2013 breach of security at a critical substation's control building, mentioned previously, which was undetected for almost 2 days. Additionally, vandalism and other physical attacks nationwide on utility facilities represented a substantial number of incidents that were reported to the Department's Office of Electricity Delivery and Energy Reliability in 2013 and 2014. Specifically, of the 388 incidents reported during the 2-year period, 151 (or 39 percent) indicated some level of physical attack.

In addition, the physical security of the bulk-power grid has long been a matter of concern for policy makers, and attention to these assets increased significantly following the 2013 physical attack on a utility's substation located in California. The attack, although it did not result in power outages, caused $15.4 million in damages to 17 transformers and 6 circuit breakers. The major risk associated with a physical attack against an electricity grid facility is that it may cause substantial damage resulting in widespread outages that last for days or weeks.

RECOMMENDATIONS

Western had taken a number of positive actions to improve the physical security at its critical assets; however, significant improvements still need to be made to reduce the risk of damage to the Nation's electric transmission system. Therefore, we recommend that the Administrator of the Western Area Power Administration:

1. Establish specific policies and procedures to implement requirements in WAPA Order 470.1H to ensure:

   a. Minimum security requirements are met at all of Western's critical assets;
   b. Maintenance and replacement of security measures are made a priority and completed; and
   c. Access keys to critical substation gates and control houses are accounted for and maintained by authorized personnel.

2. Establish corrective action plans containing statuses, decisions, and justifications, to ensure that physical security measures identified in risk assessments are addressed.

3. Create a formal funding plan and process to ensure recommended physical security measures are prioritized and funded.

4. Implement a performance assurance program to ensure that physical security measures are performing as designed at all critical assets, consistent with Department and Department of Homeland Security policies.

MANAGEMENT RESPONSE

Western concurred with the recommendations and indicated that corrective actions were planned to address the identified issues. Western stated that it was refining its policies and procedures to conform to accepted practices for implementing requirements contained in WAPA Order 470.1H. Western also stated that it had implemented a two-phased approach to complete corrective action plans for its critical assets by June 2016. Additionally, Western stated that it was establishing a formal process to capture and document criticality, prioritization, funding, and project timelines and was developing a formal performance assurance plan in accordance with Department and Western policies. Western's formal comments are included in Appendix 3.

AUDITOR COMMENTS

Western's comments and corrective actions are responsive to our recommendations.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether Western Area Power Administration (Western) had effectively and efficiently managed the protection of its critical assets.

Scope

The audit was performed from October 2014 to April 2016, at Western's Headquarters office in Lakewood, Colorado. Site visits were conducted at two of Western's four regions. The audit was conducted under Office of Inspector General project number A15DN004.

Methodology

To accomplish our audit objective, we:

- Reviewed pertinent laws and regulations related to the identification and protection of critical assets;

- Reviewed Western, Department of Energy, North American Electric Reliability Corporation, and other Federal agency policies and procedures;

- Reviewed prior Office of Inspector General and Government Accountability Office reports (as part of our review of Office of Inspector General reports, we evaluated whether recommendations from our 2010 Audit Report on *Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations—Follow-up Audit* (DOE/IG-0842, October 2010) were addressed and implemented);

- Interviewed the regional officials responsible at Western for identifying and securing critical assets, as well as maintaining and testing physical security measures;

- Interviewed the Office of Security and Emergency Management officials at Western that are responsible for establishing security policies and procedures and implementing physical security and risk assessments' processes;

- Conducted site visits at regions and observed the physical security measures in place at five substations and one control center; and

- Analyzed completion of risk assessments performed at the regions since our prior audit.

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, we assessed significant internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the implementation of the *GPRA Modernization Act of 2010* and found that Western had established performance measures specifically related to the protection of critical 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. Finally, we did not rely on computer-processed data to achieve our audit objective and, therefore, did not conduct a reliability assessment of computer-processed data.

An exit conference was held with Western officials on March 16, 2016.

PRIOR REPORTS

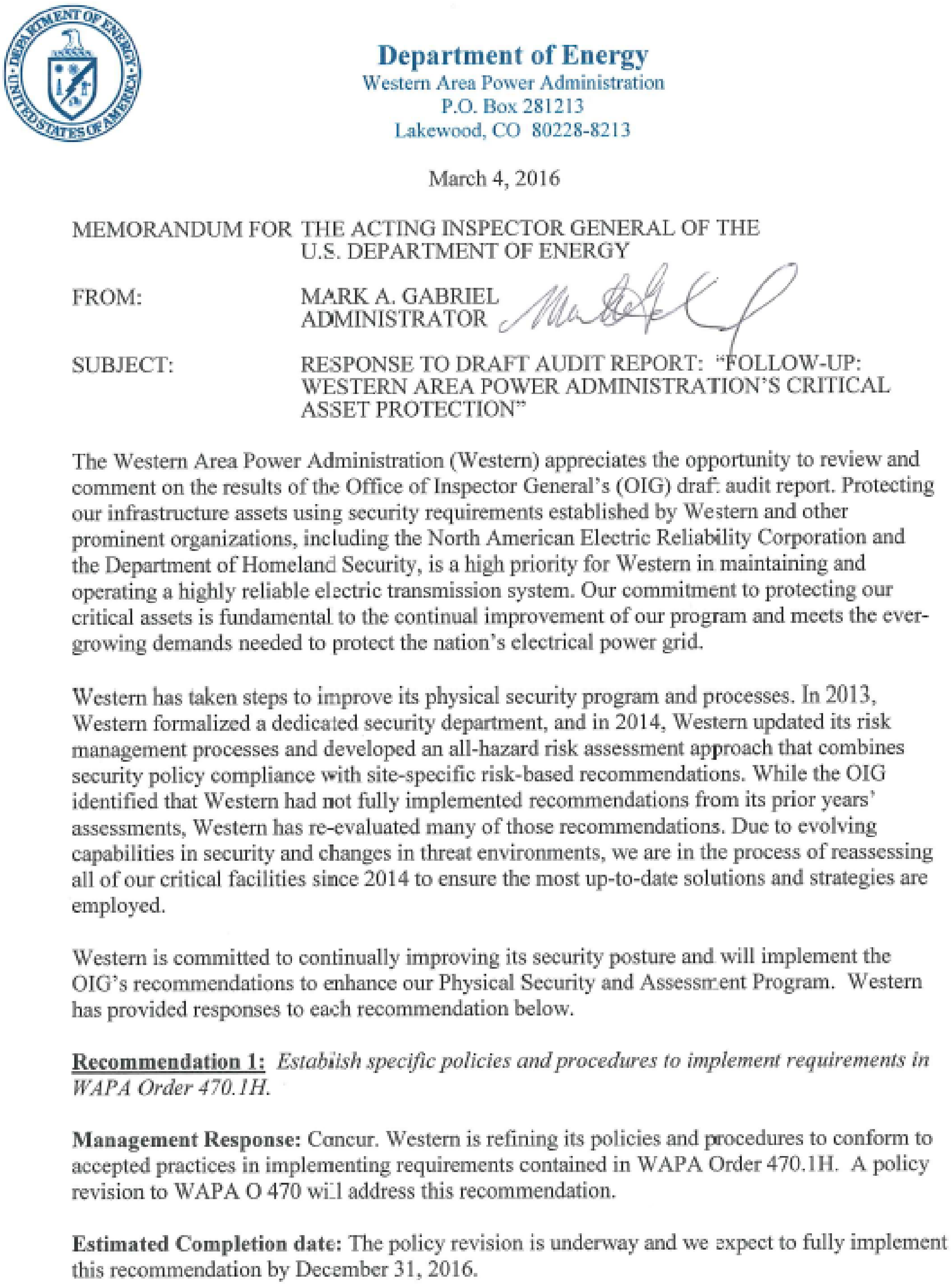
- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2015* (DOE/IG-0924, October 2014). The Department of Energy, Office of Inspector General, identifies what it considers to be the most significant management challenges facing the Department each year. The overall goal is to focus attention on significant issues with the objective of working with Department managers to enhance the effectiveness of agency programs and operations. According to the report, safeguards and security remained on the list of management challenges for fiscal year 2015.

- Audit Report on *Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations–Follow-up Audit* (DOE/IG-0842, October 2010). This audit found that the Power Marketing Administrations' efforts essential to identifying current risks or threats and mitigating those risks remained incomplete at the time of the audit. While a number of activities relevant to critical infrastructure protection had been initiated, the Power Marketing Administrations had not completed and updated, when appropriate, all required vulnerability and risk assessments. It also had not conducted required tests to ensure that security measures for physical assets were operating as designed. The audit also found that Bonneville Power Administration (Bonneville) and Western Area Power Administration (Western) had not implemented security enhancements recommended in completed risk assessments. Specifically, neither Bonneville nor Western had implemented electronic perimeter intrusion motion detection and alarm systems to protect critical assets as recommended in the assessments.

- Audit Report on *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003). This report disclosed concerns regarding the Power Marketing Administrations' critical asset assessment efforts. The report found that Bonneville had conducted adequate vulnerability and risk assessments for its most critical assets; however, Western and Southwestern Power Administration (Southwestern) assessments were either inadequate or did not exist. The report recommended that Western and Southwestern conduct vulnerability and risk assessments on their critical assets.

APPENDIX 3

MANAGEMENT COMMENTS



Department of Energy
Western Area Power Administration
P.O. Box 281213
Lakewood, CO 80228-8213

March 4, 2016

MEMORANDUM FOR THE ACTING INSPECTOR GENERAL OF THE U.S. DEPARTMENT OF ENERGY

FROM: MARK A. GABRIEL
ADMINISTRATOR

SUBJECT: RESPONSE TO DRAFT AUDIT REPORT: "FOLLOW-UP: WESTERN AREA POWER ADMINISTRATION'S CRITICAL ASSET PROTECTION"

The Western Area Power Administration (Western) appreciates the opportunity to review and comment on the results of the Office of Inspector General's (OIG) draft audit report. Protecting our infrastructure assets using security requirements established by Western and other prominent organizations, including the North American Electric Reliability Corporation and the Department of Homeland Security, is a high priority for Western in maintaining and operating a highly reliable electric transmission system. Our commitment to protecting our critical assets is fundamental to the continual improvement of our program and meets the ever-growing demands needed to protect the nation's electrical power grid.

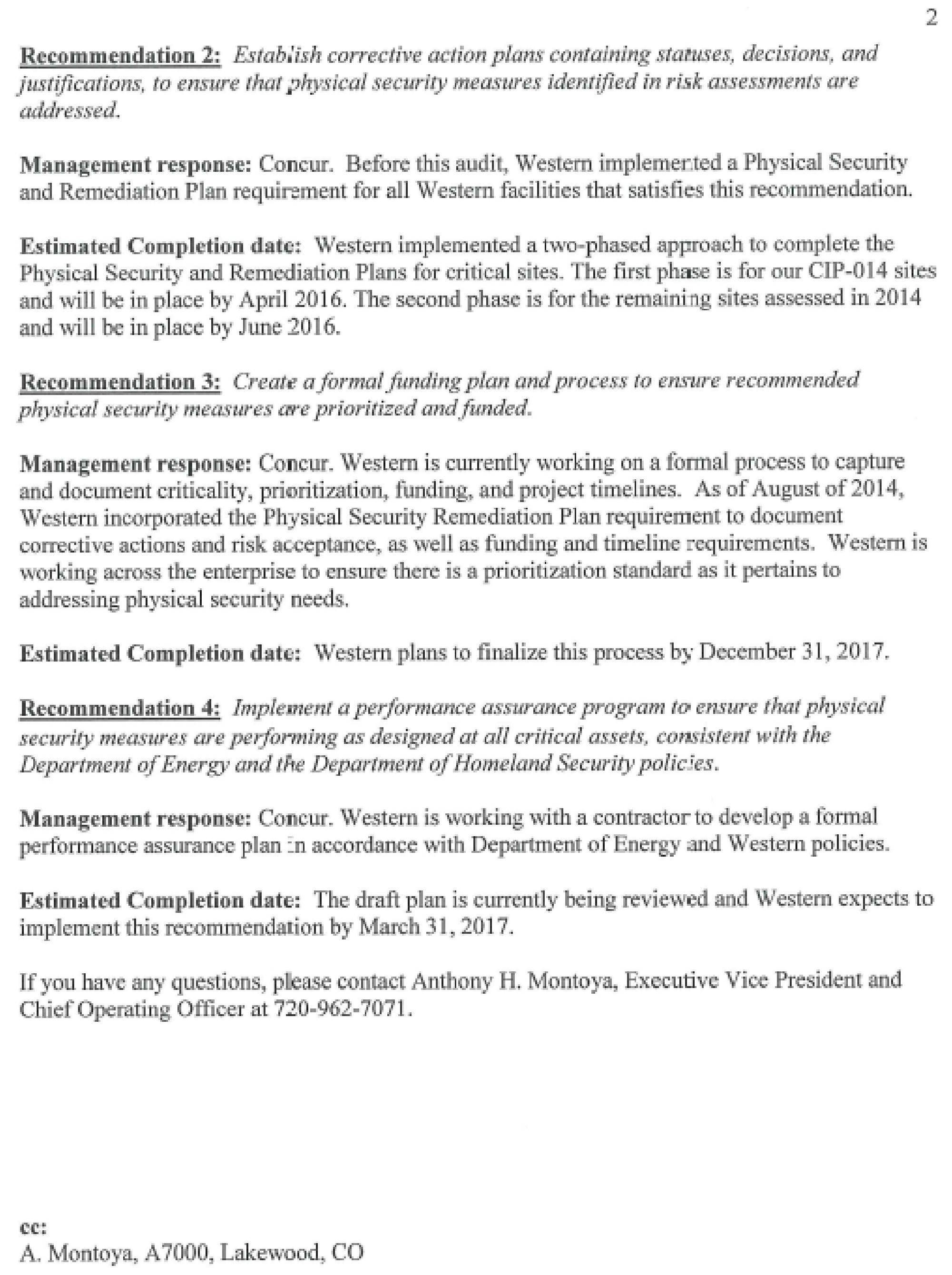
Western has taken steps to improve its physical security program and processes. In 2013, Western formalized a dedicated security department, and in 2014, Western updated its risk management processes and developed an all-hazard risk assessment approach that combines security policy compliance with site-specific risk-based recommendations. While the OIG identified that Western had not fully implemented recommendations from its prior years' assessments, Western has re-evaluated many of those recommendations. Due to evolving capabilities in security and changes in threat environments, we are in the process of reassessing all of our critical facilities since 2014 to ensure the most up-to-date solutions and strategies are employed.

Western is committed to continually improving its security posture and will implement the OIG's recommendations to enhance our Physical Security and Assessment Program. Western has provided responses to each recommendation below.

Recommendation 1: *Establish specific policies and procedures to implement requirements in WAPA Order 470.1H.*

Management Response: Concur. Western is refining its policies and procedures to conform to accepted practices in implementing requirements contained in WAPA Order 470.1H. A policy revision to WAPA O 470 will address this recommendation.

Estimated Completion date: The policy revision is underway and we expect to fully implement this recommendation by December 31, 2016.



Recommendation 2: *Establish corrective action plans containing statuses, decisions, and justifications, to ensure that physical security measures identified in risk assessments are addressed.*

Management response: Concur. Before this audit, Western implemented a Physical Security and Remediation Plan requirement for all Western facilities that satisfies this recommendation.

Estimated Completion date: Western implemented a two-phased approach to complete the Physical Security and Remediation Plans for critical sites. The first phase is for our CIP-014 sites and will be in place by April 2016. The second phase is for the remaining sites assessed in 2014 and will be in place by June 2016.

Recommendation 3: *Create a formal funding plan and process to ensure recommended physical security measures are prioritized and funded.*

Management response: Concur. Western is currently working on a formal process to capture and document criticality, prioritization, funding, and project timelines. As of August of 2014, Western incorporated the Physical Security Remediation Plan requirement to document corrective actions and risk acceptance, as well as funding and timeline requirements. Western is working across the enterprise to ensure there is a prioritization standard as it pertains to addressing physical security needs.

Estimated Completion date: Western plans to finalize this process by December 31, 2017.

Recommendation 4: *Implement a performance assurance program to ensure that physical security measures are performing as designed at all critical assets, consistent with the Department of Energy and the Department of Homeland Security policies.*

Management response: Concur. Western is working with a contractor to develop a formal performance assurance plan in accordance with Department of Energy and Western policies.

Estimated Completion date: The draft plan is currently being reviewed and Western expects to implement this recommendation by March 31, 2017.

If you have any questions, please contact Anthony H. Montoya, Executive Vice President and Chief Operating Officer at 720-962-7071.

cc:
A. Montoya, A7000, Lakewood, CO

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.