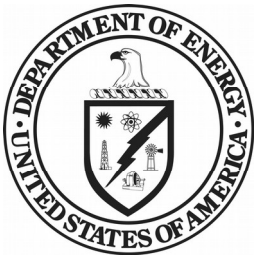

U.S. Department of Energy
Office of Inspector General
Office of Audits & Inspections

Audit Report

Management of Western Area Power Administration's Cyber Security Program

DOE/IG-0873 October 2012

Department of Energy
Washington, DC 20585

October 22, 2012

MEMORANDUM FOR THE UNDER SECRETARY OF ENERGY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Western Area Power Administration's Cyber Security Program"

INTRODUCTION AND OBJECTIVE

The Department of Energy's Western Area Power Administration (Western) markets and delivers hydroelectric power and related services to 15 states within the central and western United States. As the largest U.S. Power Marketing Administration, millions of households and businesses count on Western for low cost, reliable electric prower. To successfully transmit hydroelectric power to customers and local utilities within its territory, Western relies on a number of information systems that support the operation, maintenance and management of a massive electrical power complex, as well as financial and administrative activities.

Prior Office of Inspector General (OIG) reports identified weaknesses related to the management of information technology programs and infrastructure at Western and other Federal Power Marketing Administrations. For example, our review of *Cyber Security Risk Management Practices at the Southeastern, Southwestern and Western Area Power Administrations* (DOE/IG-0805, November 2008) revealed that the Administrations did not always develop adequate security plans, test physical and cyber security controls, resolve identified cyber security weaknesses or ensure that systems could be recovered in the event of a significant outage. Cyber security and the protection of the U.S. vital infrastructure are current topics of prime interest. Consequently, we initiated this follow-up audit to determine whether Western effectively and efficiently implemented its cyber security program.

RESULTS OF AUDIT

Western had made a number of enhancements to its cyber security program since our prior review. However, we identified several weaknesses related to vulnerability management and security controls that could negatively impact its cyber security posture. Specifically, Western had not always implemented cyber security controls designed to address known system vulnerabilities and ensured that access controls designed to protect its information systems and data were in place. In particular:

- We found that nearly all of the workstations we tested contained at least one high-risk vulnerability related to software updates or patches. Specifically, we identified 19 software applications installed on workstations that were not configured with the latest

version or were missing security updates, including applications supporting office automation, project management and multimedia functions;

- During internal vulnerability scanning, we found that a network server was running an unsupported version of a software application. While the application had been removed by Western as a result of our testwork, a successful attack on this type of known high-risk vulnerability could have put the affected server at risk, potentially causing a disruption to normal business operations. We also identified 30 network servers that contained vulnerabilities that could have been made more secure by applying publicly available security patches and updates;

- External vulnerability testing revealed a public-facing application server that was configured with a default username and password. This high-risk weakness could have allowed an attacker with an Internet connection to obtain unauthorized access to an internal database supporting the electricity scheduling system; and,

- Our testing of cyber security controls identified weaknesses related to access security controls. In particular, we noted a deficiency related to account management for two of the four systems reviewed.

The weaknesses identified occurred, in part, because Western had not always implemented policies and procedures related to vulnerability and patch management. Specifically, while cyber security officials conducted regular scans on two of the systems reviewed, they did not always identify and correct known vulnerabilities. For instance, the external vulnerability we discovered during testing was likely not identified because Western's scan profiles were configured to run a less intrusive scan than typical to avoid negatively impacting system performance. In addition, officials had not fully implemented policies and procedures related to managing access to systems and information, including deactivating and/or disabling unneeded user accounts in a timely manner. Implementation of controls such as those included in our testwork is an important element of an effective risk management and continuous monitoring process.

Western had taken action to address many of the vulnerabilities identified during our testing. In some instances, management was aware of the identified vulnerabilities and was in the process of upgrading systems, procuring new devices or virtualizing servers to correct the issues. However, in our view, Western's systems remain at a higher than necessary level of risk of attack until these vulnerabilities are fully remediated and control procedures are in place to ensure that applications and programs are updated in a timely manner. As such, we have made recommendations that should assist in strengthening Western's cyber security posture.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had, in some cases, already completed actions to address specific weaknesses identified in our report. In other instances, management commented that it was in the process of implementing program improvements to address our recommendations. Management's formal comments are included in Appendix 3.

Attachment

cc: Deputy Secretary
Associate Deputy Secretary
Administrator, Western Area Power Administration
Chief of Staff
Chief Health, Safety and Security Officer
Chief Information Officer

REPORT ON MANAGEMENT OF WESTERN AREA POWER ADMINISTRATION'S CYBER SECURITY PROGRAM

TABLE OF CONTENTS

MANAGEMENT OF WESTERN AREA POWER ADMINISTRATION'S CYBER SECURITY PROGRAM

CYBER SECURITY

The Western Area Power Administration (Western) had made a number of enhancements to its cyber security program since our review of *Cyber Security Risk Management Practices at the Southeastern, Southwestern and Western Area Power Administrations* (DOE/IG-0805, November 2008). For instance, Western officials commented that they enhanced control testing through regular Security Test and Evaluation reviews and automated security scanning. Our current review, however, identified several cyber security related weaknesses that could negatively impact Western's information security posture. Specifically, we found that Western had not always implemented cyber security controls designed to address known system vulnerabilities and deployed access controls designed to protect its information systems and data. We also identified weaknesses related to controlling user access to two of the four systems reviewed.

Vulnerability Management

Our vulnerability testing of select Western information systems identified internal and external vulnerabilities related to server and workstation configuration management, software management and access controls that could be exploited by an attacker to compromise systems and data. Internal vulnerability scanning was performed on three information systems supporting Western's business functions related to financial management, power management and general support. During our internal vulnerability scanning, significant high-risk weaknesses were identified using authenticated and unauthenticated scanning techniques. Authenticated scanning utilizes login names and passwords to simulate a user being on the system. In contrast, unauthenticated scanning does not make use of login credentials and is used to identify basic network setting vulnerabilities. In particular:

- We found that nearly all of the 105 workstations tested contained at least 1 high-risk vulnerability related to software updates or patches. In particular, we identified 19 software applications, supporting functions such as office automation, multimedia and project management that were not configured with the latest version of the application or were missing security updates that were older than 3 months. While management agreed with our findings, it commented that certain vendors issue large numbers of security patches at irregular intervals, making them difficult to manage. By exploiting several vulnerable desktop

applications, a knowledgeable individual could obtain unauthorized access to Western workstations from the internal network or any external Internet connection;

- During authenticated scanning, we found that a network server was running an unsupported version of a software application. The application was removed by Western personnel as a result of our testing. However, a successful attack on this type of known high-risk vulnerability could have put the affected server at risk for remote code execution and other vulnerabilities that could disrupt normal business operations; and,

- Our unauthenticated scanning identified 30 network servers that contained vulnerabilities that could have been remediated by installing readily available security patches and updates. At the time of our testing, a program installed on 29 devices was affected by multiple high-risk vulnerabilities. Western personnel had taken action to address this weakness and provided evidence that the latest version of the program offered by the vendor had been installed on each of the identified devices. Exploitation of this type of vulnerability, however, could have allowed an attacker to gain unauthorized access to internal devices and sensitive data.

We also conducted external vulnerability testing that revealed a high-risk weakness relating to ineffective access controls. Specifically, we identified an externally facing application server that was configured with a default username and password. This high-risk vulnerability could have been exploited by an attacker from any Internet connection to obtain unauthorized access to the internal database supporting the electricity scheduling system. In addition, Western's workstations and those of its customers could also have been compromised by this vulnerability. To its credit, Western personnel took immediate action to correct this weakness during our testing.

System Access Controls

Our testing of cyber security controls also identified weaknesses related to access controls over various information systems. In particular, we identified weaknesses related to account management for two of the four systems we reviewed, including those supporting power maintenance and scheduling. Specifically, we found that system access was not always revoked for

terminated or separated users, including a total of five separated users that remained on active user lists subsequent to departure, even though Western had a requirement that user accounts be blocked according to an employee's departure date. Four of the five users had access to Western's power maintenance system. In another instance, a former employee had been retired for more than a year and yet still had access to the scheduling system. Federal guidance suggests that accounts for separated and terminated users be disabled or removed in a timely manner to prevent unauthorized access to critical or sensitive resources and information. Absent effective implementation of access controls, Western's systems and information could be susceptible to unauthorized use or alteration.

Patching Implementation and Policies and Procedures

The weaknesses identified were due, in part, to ineffective implementation of policies and procedures related to vulnerability and patch management. Even when certain practices were implemented, the practices were not always documented. In addition, officials had not fully implemented policies and procedures related to managing access to systems and information. Effective implementation of procedures and the ability to document processes and risk-based decisions are important elements to help ensure that risk management and continuous monitoring processes are effective.

Vulnerability and Patch Management

While cyber security officials conducted monthly authenticated and quarterly unauthenticated scans on two of the systems reviewed, they did not always identify and correct known vulnerabilities. For instance, the external vulnerability found during testing was likely not identified because Western's scan profiles were configured to run a less intrusive scan than typical to avoid bringing down the system. Western officials stated that they have since edited their methodology and reconfigured profiles to help discover the type of weaknesses identified during our testing.

Although Western had processes in place for identifying and remediating vulnerabilities, officials had not formally documented the practices associated with the vulnerability and patch management program at the time of our review. Notably, new scanning procedures for Western and its regional offices were being developed. Officials stated that the procedures will include requirements for the frequency of scanning, a timeline for remediation of identified vulnerabilities and risk acceptance procedures. In addition, Western officials stated that they were previously aware of many of the vulnerabilities that were identified and had accepted the risk of the weaknesses. While management

provided sufficient documentation to support its assertion in some cases, in other instances supporting documentation for a risk analysis was either not provided or was inadequate. Without an adequate and supportable assessment of risk, senior managers and other officials may lack the necessary information to make decisions essential to determining whether not remediating known vulnerabilities is appropriate and yields benefits greater than the risk of compromise.

Implementation of Access Controls

Western officials had not fully implemented policies and procedures related to controlling user access to systems and data. For instance, system administrators did not always follow organization policy for deactivating or disabling accounts according to the employee's departure date. Furthermore, contrary to recommendations from the National Institute of Standards and Technology (NIST), Western relied on manual rather than automated processes to support account management activities. Specifically, for information systems with high and moderate security categorizations such as those reviewed at Western, NIST suggests employing automated mechanisms for the deactivation of accounts that have been inactive for an established period of time. Failure to implement these access security controls could result in a knowledgeable individual using information technology resources for unauthorized and sometimes malicious purposes that may be detrimental to Western's operations.

Information Systems at Risk

Without improvements to its cyber security program, Western's systems and information continue to be at a higher than necessary risk from internal and external threats. As noted, many of the vulnerabilities we identified created the potential for an attacker to gain unauthorized access to networks, workstations and devices, increasing the risk of compromise, loss, modification and non-availability. Any disruption of service resulting from compromised or affected systems could significantly impact critical business functions and Western's mission of delivering reliable, cost-based hydroelectric power to its customers.

RECOMMENDATIONS

To improve the effectiveness of Western's cyber security program, we recommend that the Administrator, Western Area Power Administration:

1. Implement appropriate controls to correct the specific cyber security weaknesses identified in this report;

2. Ensure that policies and procedures are developed, as needed, and are effectively implemented to enhance vulnerability and patch management practices; and,

3. Effectively implement policies related to access controls, including deactivating and/or disabling user accounts in a timely manner.

MANAGEMENT REACTION

Management concurred with the report's findings and recommendations and commented that corrective actions had been taken or were planned to address the issues identified. Management stated that the majority of desktop vulnerabilities identified were a result of outdated patches relating to a specific application. Management commented that the patches for this application were released at irregular intervals, making it difficult to immediately apply all newly released patches. Management stated that it had accepted and documented this weakness as a business risk at Western. In addition, management commented that the majority of the vulnerable servers identified in our report were a result of vendors not supplying security patches and believed that certain server vulnerabilities identified in our report were false positives.

AUDITOR COMMENTS

Management's comments and planned corrective actions are responsive to our recommendations. During our review, we evaluated potential compensating controls related to identified vulnerabilities and only reported on vulnerabilities for which mitigating controls were not in place or were not fully effective. In addition, we excluded vulnerabilities that were considered "false positives" and only included those for which security patches had been released by vendors at least 90 days prior to our testing. Although management stated that it had accepted and documented the risk of unpatched desktop systems, we were not provided with adequate documentation to support this assertion. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

To determine whether the Western Area Power Administration (Western) effectively and efficiently implemented its cyber security program.

SCOPE

The audit was performed between January 2012 and October 2012, at Western's Corporate Services Office in Lakewood, Colorado and Watertown Operations Office in Watertown, South Dakota. The audit included internal and external vulnerability scanning conducted by KPMG, LLP on behalf of the Office of Inspector General. We conducted external testing of networks and systems as an outsider without any elevated privileges. We conducted internal scanning as an authenticated user (a user with a valid username and password) and reported on vulnerabilities that could be exploited by both an insider and a remote attacker. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls. At the request of Western, we did not conduct vulnerability scanning on the Supervisory Control and Data Acquisition Systems because of concerns over the potential impact to operations.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal laws and regulations pertaining to information and cyber security such as the *Federal Information Security Management Act of 2002*;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology, such as NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;
- Obtained and analyzed documentation from Western pertaining to its cyber security program; and,
- Held discussions with officials from Western's Corporate Services Office and the Watertown Operations Office.

We conducted this 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 objectives. 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 to the extent necessary to satisfy the audit objective. In particular, we assessed Western's implementation of the *GPRA Modernization Act of 2010* and determined that while it did not have specific performance measures for cyber security, it had established performance measures to improve information technology policy and oversight. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our audit. We did not solely rely on computer-processed data to satisfy our objective. Computer-assisted audit tools were used to perform probes and scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

Management waived the exit conference.

PRIOR REPORTS

- Audit Report on *Management of Bonneville Power Administration's Information Technology Program* (DOE/IG-0861, March 2012). The review identified areas of concern at the Bonneville Power Administration (Bonneville) related to cyber security, project management and procurement of information technology (IT) resources. In particular, Bonneville had not implemented controls designed to address known system vulnerabilities. Operational security controls designed to protect Bonneville's systems also had not been fully implemented. It was also determined that several system development efforts suffered from cost, scope and schedule issues, and Bonneville's IT software was not always procured in a coordinated manner, resulting in increased security risks.

- Special Report on *Management Challenges at the Department of Energy – Fiscal Year 2012* (DOE/IG-0858, November 2011). On an annual basis, the Office of Inspector General (OIG) identifies what it considers to be the most significant management challenges facing the Department of Energy (Department). The identified challenges represent risks inherent in the Department's wide ranging and complex operations as well as those related to specific management processes. The OIG's management challenge list for Fiscal Year 2012 included cyber security.

- Audit Report on *The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011). The review identified various control weaknesses related to access controls, vulnerability management, integrity of web applications, contingency planning, change control management and cyber security training. In specific regards to access control, weaknesses included issues such as failure to perform management reviews of user accounts and user access privileges, default or weak usernames and passwords, segregation of duties, and a lack of logging/monitoring information system activities. Vulnerability management weaknesses consisted of varying degrees of vulnerable applications, desktops, and network systems missing security updates and/or patches for known vulnerabilities.

- Audit Report on *Cyber Security Risk Management Practices at the Southeastern, Southwestern, and Western Area Power Administrations* (DOE/IG-0805, November 2008). The audit identified several critical certification and accreditation weaknesses at Southeastern, Southwestern and Western Area Power Administrations. Specifically, it was determined that the Power Marketing Administrations (PMAs) had not always developed adequate security plans nor tested physical and cyber security controls. In addition, it was noted that the PMAs had not always developed corrective action plans necessary to resolve weaknesses. Similarly, contingency plans were not always developed to ensure that systems could be recovered in the event of a significant outage.

MANAGEMENT COMMENTS

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

SEP 19 2012

MEMORANDUM FOR RICKY R. HASS (IG-30)
DEPUTY INSPECTOR GENERAL FOR AUDITS
AND INSPECTIONS

FROM: ANITA J. DECKER
ACTING ADMINISTRATOR

SUBJECT: Response to Draft Audit Report on "Management of Western Area Power Administration's Cyber Security Program"

The Western Area Power Administration appreciates the opportunity to comment on the draft report "Management of Western Area Power Administration's Cyber Security Program". As noted in several sections of the draft report, Western has taken many positive actions to improve its cyber security practices since our last evaluation by the Inspector General. We understand the IG team's findings, appreciate the observations and recommendations, and would like to thank the auditors for assisting in the improvement of Westerns Cyber Security posture.

The auditors identified 105 workstations containing high risk vulnerabilities. The majority of these were as a result of outdated [redacted] patches. Western has a number of enterprise applications which rely on this technology. Application vendors do not coordinate their upgrades with the [redacted] patch release schedule, which is irregular. Thus it is necessary to find a common [redacted] baseline under which all applications will function - this can be as much as a year behind current releases. This is a business risk accepted and documented by Western.

The auditors also identified 30 servers containing vulnerabilities. The majority of these were due to imbedded versions of web servers or security software which were impossible to upgrade due to a lack of availability of vendor-supplied patches. Others were false positives. Appropriate evidence of this was provided to the auditors.

Two issues relating to access control were identified in the report. Western has a number of systems which use dissimilar authentication methods. Thus, the NIST recommendations on automatic notification referred to in the draft report cannot always be implemented easily. To the extent that it is technically possible it has been done.

Based on the actions taken thus far as a result of the audit, and with due consideration to the Inspector General's recommendations, we believe that Western will continue to maintain an effective security program that achieves the requirements set forth in FISMA. We remain committed to safeguarding our IT infrastructure and maintaining a robust and effective cyber security program.

With regards to the draft recommendations, Western plans to address the draft report's recommendations with program improvements to be implemented as noted in the response below. Specifically, for Recommendation #1, as noted in the report, Western has corrected the specific weaknesses identified or accepted the risk on allowing the vulnerability to remain in place. For Recommendation #2, Western will develop policies and procedures as part of the on-going implementation of Continuous Monitoring and the enhancement of the Risk Management process. These efforts will be continuing but will be largely in place by December 31, 2012. With regard to Recommendation #3, for those systems and access control issues not subject to native automation, Western is in the process of implementing its Identity Compliance Enforcement Reporting (ICER) tool which will alert, in a more timely fashion, managers upon an employee departure or status change. This is expected to provide additional assurance in this matter. This also is planned for a phased implementation beginning in January 2013.

If you have further questions, please contact Eun Moredock, Chief Information Officer at 720-962-7238.

cc: Chief Information Officer, Western Area Power Administration
Compliance and Audit Liaison Manager, Western Area Power Administration
Director, Office of Financial Risk, Policy and Controls, CF-50
Assistant Director, Office of Financial Risk, Policy and Controls, CF-50
Team Leader, Office of Financial Risk, Policy and Controls, CF-50
Audit Resolution Specialist, Office of Financial Risk, Policy and Controls, CF-50
Audit Liaison, Office of the Chief Information Officer, IM-10
Audit Liaison, Western Area Power Administration, Forrestal

IG Report No. DOE/IG-0873

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report that would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

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

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://energy.gov/ig

Your comments would be appreciated and can be provided on the Customer Response Form.