OFFICE OF INSPECTOR GENERAL

U.S. Department of Energy

AUDIT REPORT

DOE-OIG-17-06 August 2017

FOLLOWUP ON BONNEVILLE POWER ADMINISTRATION'S CYBERSECURITY PROGRAM

Department of Energy
Washington, DC 20585

August 16, 2017

MEMORANDUM FOR THE SECRETARY

FROM: April Stephenson
Acting Inspector General

SUBJECT: INFORMATION: Audit Report on the "Followup on Bonneville Power Administration's Cybersecurity Program"

BACKGROUND

The Bonneville Power Administration (Bonneville) was established in 1937 as a Federal nonprofit power marketing administration and provides approximately 28 percent of the electric power used across 300,000 square miles in the Pacific Northwest. Although Bonneville is part of the Department of Energy, it is self-funded and covers its costs by selling products and services such as wholesale electrical power from 31 Federal hydroelectric projects in the Northwest and operating and maintaining about three-fourths of the high-voltage transmission in its service territory. With an overall budget of $4.3 billion, Bonneville utilizes numerous information systems to conduct business and electricity-related operations, including financial and administrative systems. In fiscal year 2017, Bonneville budgeted more than $7 million for its cybersecurity program to protect systems that, if compromised, could have a significant impact on Bonneville and its customers.

Prior reviews have identified weaknesses related to Bonneville's cybersecurity program. For example, our report on the *Management of Bonneville Power Administration's Information Technology Program* (DOE/IG-0861, March 2012) identified cybersecurity weaknesses in areas such as access control, vulnerability management, configuration management, least privilege, and contingency and security planning. More recently, the Office of Inspector General received two allegations – one that alleged Bonneville officials had required nearly all teams to stop patching its systems and another that officials did not ensure systems stayed up-to-date on security controls. We initiated this followup audit to determine whether Bonneville effectively implemented its cybersecurity program over financial and administrative systems and to evaluate the circumstances surrounding the allegations.

RESULTS OF AUDIT

While we did not substantiate all information included in the allegations, we did identify various weaknesses related to vulnerability management similar to those included in the allegations.

Specifically, we were unable to substantiate that Bonneville required officials to stop patching systems. However, we did note that officials had not ensured all systems contained up-to-date security controls. Notably, Bonneville made efforts to improve its cybersecurity program since our prior review such as elevating the Chief Information Officer position for greater visibility, accountability, and oversight. However, we found that Bonneville had not implemented a fully effective cybersecurity program and continued to identify weaknesses in the areas of access controls, vulnerability and configuration management, and contingency planning. We also noted weaknesses related to risk management. In particular, we identified the following:

- Bonneville had not implemented effective risk management practices as part of its security planning process. In particular, Bonneville had not ensured that system security plans were complete and accurate. For instance, the security plans reviewed did not include updated Federal cybersecurity controls related to access control, configuration management, and security assessments and authorization. Furthermore, we identified weaknesses related to Bonneville's process for authorizing systems to operate. Specifically, although a Bonneville official commented that weaknesses were shared verbally with the authorizing official – the Federal official responsible for granting approval to operate an information system – we found that Bonneville had not ensured all known security weaknesses were included in the security assessment documentation used to approve systems for operation. In one instance, the authorizing official approved a system for operation even though nearly one-third of the security controls had failed testing, resulting in numerous high-risk weaknesses.

- Bonneville had not fully implemented effective logical access controls. For instance, an inventory management application did not adequately protect sensitive information. We found that user credential information was not always securely stored or encrypted when transmitted on the network. In addition, contrary to Bonneville's cybersecurity policy, more than 250 user account passwords had not been changed within timeframes established by the *BPA IT Technical Architecture* and/or the Cyber Security Program Plan. Furthermore, users were not required to agree to rules of behavior prior to gaining access to Bonneville's systems, including systems that contained sensitive information.

  We also found that physical access to Bonneville's data centers was not properly monitored. In particular, visitor logs were not required or did not exist for any of Bonneville's seven data centers used to support financial and administrative functions. In addition, there may have been an excessive number of individuals with access to Bonneville's data centers. Specifically, nearly 60 percent of the more than 300 individuals granted access had never badged into their assigned data centers. As a result of our test work, Bonneville officials removed access for one individual that had not accessed the data center in 5 years. We remain concerned that the improper monitoring of physical controls within Bonneville's data centers unnecessarily increases the risk of insider threat.

- Similar to the findings from our prior report on *Management of Bonneville Power Administration's Information Technology Program*, a number of configuration management vulnerabilities existed on systems reviewed that weakened Bonneville's

security posture. In particular, Bonneville used numerous types of software applications to support both business and cybersecurity functions that were no longer supported by the vendor. In some instances, the vendor had not supported the software in several years. In addition, many servers, workstations, and applications were missing security patches or contained other significant moderate and high-risk vulnerabilities.

- Contingency planning and testing issues continued to exist at Bonneville. Similar to issues identified in our prior report, we found that contingency plans had not always been developed in a timely manner or tested for the systems reviewed. Contrary to National Institute of Standards and Technology (NIST) requirements, 9 of the 10 contingency plan test results reviewed did not provide quantifiable measures of success such as carrying out emergency procedures within prescribed timeframes. In addition, we found that one system's contingency plan was not developed until more than 3 years after the system was approved to operate.

The issues identified occurred, at least in part, because officials had not ensured that Federal and Bonneville requirements were updated and/or fully implemented. For instance, officials had not incorporated the most recent Federal requirements issued by NIST into policies and system security plans even though the requirements were issued more than 3 years prior to our review. In addition, even when policies existed related to access control, configuration management, and vulnerability management, Bonneville officials had not taken appropriate actions to ensure that the policies were fully implemented. We also determined that, contrary to Federal requirements, Bonneville had not implemented an effective continuous monitoring program. For instance, Bonneville lacked separation of duties related to the individuals that designed security controls and tested those controls. Moreover, Bonneville did not effectively utilize plans of action and milestones, a critical component of an effective continuous monitoring program. In many instances, Bonneville did not track weaknesses through plans of action and milestones or did not correct weaknesses in a timely manner. Notably, Bonneville had created a distinct remediation team dedicated to monitoring identified weaknesses, focusing on those with the highest risk.

Notably, Bonneville had taken action to enhance access controls by significantly reducing the number of local system administrators with elevated privileges since our prior review. However, without improvements to its cybersecurity program, Bonneville may continue to operate systems at a higher than necessary risk of compromise, loss, modification, and non-availability. For instance, certain vulnerabilities identified could have permitted an attacker or malicious user to make unauthorized changes to data, disclose sensitive information, or deny legitimate users access to systems supporting business operations and other general support systems. In addition, unaddressed weaknesses related to risk management and continuous monitoring will continue to contribute to vulnerable systems being approved to operate by the authorizing official. In light of the weaknesses identified, we made several recommendations that, if fully implemented, should aid officials in improving Bonneville's cybersecurity posture.

MANAGEMENT RESPONSE

Management generally concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address issues identified in the report.

Management did not concur with a portion of one recommendation concerning separation of duties, asserting that Bonneville's organizational structure sufficiently mitigated risk. Management's comments and our responses are summarized in the body of the report. Management's formal comments are included in Appendix 3.

Attachment

cc: Administrator, Bonneville Power Administration
Chief of Staff
Chief Information Officer

Followup on Bonneville Power Administration's Cybersecurity Program

TABLE OF CONTENTS

Audit Report

Appendices

Followup on Bonneville Power Administration's Cybersecurity Program

DETAILS OF FINDING

The Bonneville Power Administration (Bonneville) is a Federal nonprofit power marketing administration that provides approximately 28 percent of the electric power used across 300,000 square miles in the Pacific Northwest. Bonneville utilizes numerous information systems to conduct business and electricity-related operations, including financial and administrative systems. The *Federal Information Security Modernization Act of 2014* requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect systems and data that support the operations and assets of an agency, including those provided or managed by contractors. To facilitate satisfying the requirements, the National Institute of Standards and Technology (NIST) developed mandatory guidance for categorizing and protecting Federal information and systems according to risk levels. Our prior report on *Management of Bonneville Power Administration's Information Technology Program* (DOE/IG-0861, March 2012) identified cybersecurity weaknesses in areas such as access control, patch management, configuration management, least privilege, and contingency and security planning. In addition, the Office of Inspector General recently received two allegations concerning weaknesses related to patch and vulnerability management – one allegation that Bonneville officials had required nearly all teams to stop patching systems, the other that officials did not ensure that systems contained updated security configurations.

Bonneville had taken actions to improve its cybersecurity program since our prior review. For instance, the Office of Cyber Security increased its staff and created a group to work with system personnel in implementing corrective actions. However, we continued to identify cybersecurity weaknesses at Bonneville. Although we did not substantiate all information included in the allegations, we did identify various weaknesses related to vulnerability management similar to those included in the allegations. Our current review of three information systems and the network that supported Bonneville's business functions across numerous systems and devices found that weaknesses existed related to risk management, access controls, configuration and vulnerability management, and contingency planning.

Risk Management

Although Federal requirements directed agencies to transition from a cyclical, compliance-based information system certification and accreditation process to a more risk-based approval process, we found that Bonneville had not implemented effective risk management practices as part of its security planning process. According to NIST Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, effective security planning supports the system development life cycle and should be updated as system events trigger the need for revision to accurately reflect the most current state of the system. However, Bonneville had not ensured that system security plans were always complete and accurate. For instance, officials had not incorporated updated Federal cybersecurity requirements from NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, issued in April 2013, into any of the system security plans reviewed even though they should

have been incorporated within a year of issuance. Specifically, although Bonneville officials stated that the updated standards were used for system authorization testing, officials had not incorporated more than 40 controls and control enhancements into system security plans or the control testing in areas such as identification and authentication controls, access controls, and configuration management that were included in the latest Federal requirements. In addition, although Bonneville officials commented that information system owners were responsible for maintaining the security plans, we found that each of the system security plans reviewed referenced outdated policies or procedures. Furthermore, control descriptions included in security plans were inaccurate and contradicted actual responsibilities and practices at Bonneville. For example, some controls identified that a specific group was responsible for ensuring implementation of those controls; however, our discussions with officials from the referenced group indicated that they did not have responsibility for implementation of those controls.

Bonneville's security authorization packages did not include all of the information necessary to maintain adequate visibility into the cybersecurity program. Specifically, Federal cybersecurity standards required an authorizing official – a senior Federal official with the authority to assume responsibility for operating an information system at an acceptable level of risk – to explicitly accept known risks to an information system based on a review of the system security plan, security assessment report, and plan of action and milestones (POA&M). A security plan identifies how a system implements controls, a security assessment report identifies known weaknesses, and a POA&M tracks corrective actions for those identified weaknesses. A Bonneville official commented that weaknesses were verbally shared with the authorizing official. However, none of the Bonneville security assessment reports reviewed identified all control weaknesses for the authorizing official to consider when permitting the systems to operate. In one instance, the authorizing official approved a general support system for operation even though 84 of 278 (30 percent) security controls had failed, including 18 resulting in high-impact weaknesses. However, only two of the failed controls were included in the security assessment report provided to the authorizing official, both of which were low risk. The remaining 82 weaknesses were not included in the assessment report, which could have provided the authorizing official with more information to use when deciding to support operation of the system.

Access Controls

Bonneville had not fully implemented effective logical access controls over its information systems. For instance, we determined that an inventory management application did not adequately protect sensitive information such as user credentials (username and password). Specifically, the credentials were not sufficiently secured, leaving them vulnerable to being exposed to unauthorized individuals. Moreover, the inventory management application inappropriately transmitted credentials on the network without the use of encryption. In addition, more than 250 user account passwords had not been changed within timeframes established by the *BPA IT Technical Architecture* and the Cyber Security Program Plan. Although Bonneville officials explained that accounts were inactive if account passwords exceeded 90 days, we found that 38 accounts were accessed even though the passwords exceeded the time requirement. Similar to a prior weakness identified in our report on

Management of Bonneville Power Administration's Information Technology Program, our technical testing determined that weak passwords continued to exist on Bonneville's business systems. For example, six web management interfaces employed devices that used default passwords, making it easier to access the devices. Furthermore, a vulnerability existed on multiple servers that, if exploited, could have allowed a remote attacker to obtain password information from valid user accounts, potentially allowing access to the system.

Contrary to Federal requirements, users were not required to agree to rules of behavior prior to gaining access to Bonneville's systems, including systems that contained sensitive information. NIST Special Publication 800-53, Revision 4 and Office of Management and Budget Circular A-130, *Managing Information as a Strategic Resource*, required rules of behavior of individuals with access to Federal information systems, with the Circular including the consequences of behavior not consistent with the rules. NIST also required that the rules contain a signature page for each user to acknowledge receipt, indicating that they had read, understood, and agreed to abide by the rules of behavior. Bonneville officials noted that the initial logon served as the rules of behavior for all systems. However, we found that the initial logon simply noted that the user's computer system was provided for official business purposes only and that all use must be in accordance with laws, requirements, policies, and procedures.

We also found that Bonneville did not effectively monitor physical access to its data centers. While certain controls were in place, Bonneville only used a visitor log for one of seven data centers in its Portland, Oregon facility at the time of our review. However, data center officials did not always require visitors sign the log. Officials indicated a review of data center access occurred through electronic mail and relied on individuals to self-report when they no longer needed access. However, Bonneville officials had not formally maintained these reviews. In one instance, our testing identified an individual from another Federal agency had access to Bonneville's data centers for 5 years despite having never accessed the data centers, but Bonneville officials were unable to explain why reviews had not identified this person previously. In addition, nearly 60 percent of the more than 300 individuals granted access had never badged into their assigned data centers. A Bonneville official noted various reasons for access such as rotating on-call schedules and potential emergencies as justification for the additional employees. While we agree such access may be necessary, best practices noted that access should be restricted to those who need to maintain the servers or infrastructure of the room. Furthermore, we observed that most of the server racks were unlocked, a failed control that could have helped mitigate the risks associated with granting/logging access. We are concerned that without formal access reviews and additional security controls within the data centers, Bonneville may place its systems and information at an unnecessary higher risk of loss or disclosure to insider threats.

Configuration and Vulnerability Management

We identified a number of weaknesses related to missing security patches; however, we were unable to substantiate an allegation that Bonneville officials had required all teams except one to stop patching information systems. Although Bonneville officials noted improvements to its patch management program as a corrective action to recommendations from our prior review, including consolidating vulnerability management efforts under one group, we partially

substantiated an allegation that the number of missing patches was very high and found numerous servers, workstations, and applications that were missing security patches or contained other significant vulnerabilities. In addition, although Bonneville officials noted compensatory controls were in place as part of its defense-in-depth approach, our review determined additional action was necessary to improve Bonneville's security posture. Specifically, almost 480 commercial off-the-shelf products were missing patches for vulnerabilities rated as critical or high risk that were released more than 30 days prior to our scanning. In addition, one device was running an outdated software version that could have allowed an authenticated attacker[1] to bypass controls and access higher-privileged functions that are normally restricted only to administrative users.

Scanning conducted on Bonneville's systems also identified nearly 40 unsupported software applications on more than 600 network devices used to support both business and cybersecurity functions. In some instances, the vendor had not supported the software for several years. For example, one server application utilized by Bonneville had not been supported by the vendor since 2009. Prior audits have identified similar issues with the Department of Energy's software management. For example, *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013) illustrated how Department elements failing to adequately manage software resulted in the loss of more than 100,000 individuals' personally identifiable information. Considering both this and our prior Bonneville review found issues with lifecycle management, we are concerned that the appropriate action may not be taken to replace operating systems nearing end-of-life that support Bonneville's mission.

In addition, we could not substantiate all information related to a separate allegation we received of a specific system. In particular, the allegation referred to a configuration issue on a specific server that provided the ability to utilize a string of characters created to hide a user's password as a means of gaining access to the system for which the password was created. While we did not identify the specific weakness noted in the allegation, we found that Bonneville had various weaknesses related to vulnerability management. For example, six weaknesses left nearly 1,400 servers susceptible to man-in-the-middle attacks, which allows an attacker the ability to alter communication between two parties who believe they are directly communicating with each other.

Contingency Planning

Contingency planning and testing continued to be an issue for Bonneville. Our prior audit report on *Management of Bonneville Power Administration's Information Technology Program* noted that contingency plans had not always been developed or tested on the systems reviewed. An information system contingency plan provides established procedures for the assessment and recovery of a system following a disruption. The contingency plan provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. Contrary to NIST requirements, 9 of the 10 contingency plan test results reviewed did not provide quantifiable measures of success such as carrying out emergency procedures within prescribed timeframes.

[1] An authenticated attacker is one who has access to the system being exploited.

For example, our review found that half of the contingency plan tests reviewed limited exercises to either a general orientation or a review of the clarity, accuracy, and level of detail of the plans but did not include substantive, quantifiable tests that could have determined whether a contingency plan was successful. As a result, we do not believe these were true contingency plan tests but rather policy reviews. The remaining tests were operational in nature, but only a portion of one test required using the plan to rebuild a system within a set number of changes. In addition, one system's contingency plan was developed more than 3 years after the system was approved to operate.

Federal and Bonneville Requirements and Monitoring

The identified weaknesses occurred, at least in part, because officials had not updated and/or implemented Federal and Bonneville requirements. For example, Bonneville management had not included the latest revision of the NIST security control requirements into cybersecurity policies and system security plans. In addition, Bonneville policies included conflicting requirements that contributed to some of the weaknesses identified during our review. Furthermore, we identified weaknesses related to Bonneville's monitoring of cybersecurity activities.

Federal and Bonneville Requirements

Although recommended in our prior report, officials had not ensured that Federal and Bonneville cybersecurity requirements were updated and/or fully implemented. Under a risk-based cybersecurity framework that encourages the implementation of continuous system authorization, coupled with a rapidly evolving threat environment, it is important that organizations such as Bonneville fully implement required controls. However, we found that although agencies were required to implement revised NIST requirements within 1 year of the release date, Bonneville had not taken adequate action to incorporate the updated controls into policies and procedures. Although management told us that control testing included the updated NIST requirements, we found that it continued to use outdated requirements even though updated controls were issued more than 3 years prior to our review. As a result, a number of the weaknesses identified could have been addressed had management updated and implemented policies and procedures in a timely manner. Furthermore, Bonneville had not taken steps to ensure that it fully implemented NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The guide required that the security assessment reports were to include all of the controls that failed testing as well as recommendations for remediation. However, as previously noted, Bonneville had not included all failed controls in the security assessment reports for the systems reviewed. A Bonneville official stated that although discussions between security control assessors and Information System Security Officers determine which vulnerabilities result in POA&Ms and potential remediation efforts, the discussions were not documented.

Even when policies existed, Bonneville officials had not updated or fully implemented controls related to access controls and configuration and vulnerability management. For example, although Bonneville developed overarching access control policies, it did not adequately maintain a version control to determine which policy should be implemented. Specifically, we

identified conflicting Bonneville policies related to the maximum life of a user password before it had to be changed. Although the Cyber Security Program Plan (December 2015) required password changes after 60 days, the *BPA IT Technical Architecture* (revised in September 2015) required password changes after 90 days. Bonneville officials commented that version controls did not always exist, which may have contributed to the password weaknesses identified in our report.

Bonneville developed a control to periodically review baseline configurations – minimum security settings for operating systems – and publish those configurations internally. However, even though the underlying benchmark Bonneville used for its network configurations was updated in July 2015, officials continued to operate using the outdated network configuration baselines. According to Bonneville's own standard to maintain an up-to-date, complete, and accurate baseline, the outdated baselines should have been updated to reflect the most recent published configurations. Furthermore, while Bonneville continued to operate unsupported operating systems, it did not publish baselines for those systems. In particular, an operating system that supported 53 servers at Bonneville did not have a current baseline internally published and vendor support was no longer available for the operating system. Accordingly, no new security patches would be released for these antiquated systems.

Monitoring of Cybersecurity Practices

We also identified weaknesses related to Bonneville's monitoring of cybersecurity activities. Contrary to Federal requirements, we found that Bonneville had not implemented an effective continuous monitoring program. For instance, we noted a lack of separation of duties related to the individuals that designed and tested security controls. Specifically, the Office of Cyber Security was responsible for reviewing and approving system security plans and implementing the controls included in the plans. The same office also tested the controls, tracked remediation efforts for vulnerabilities, and authorized a number of information systems. Management noted that separate teams were responsible for identifying and tracking weaknesses but these teams existed within the same office. We are concerned with one office having so many responsibilities, especially in light of our findings that the authorizing official had not received all information necessary to make appropriate risk-based authorization decisions.

Bonneville also had not effectively used POA&Ms, a critical component of an effective continuous monitoring program. In many instances, Bonneville did not correct weaknesses in a timely manner. For example, although Bonneville established nearly 600 POA&M items since 2011, we found that approximately 400 of the weaknesses remained uncorrected at the time of our review. In fact, Bonneville identified more than half of the weaknesses prior to 2014, including a number of high-risk items. In addition, despite our prior recommendation to remediate previously identified weaknesses, Bonneville had not corrected two technical vulnerabilities identified during our prior review. Specifically, one vulnerability noted in our prior review could have allowed an attacker to take complete control of the affected device, but had not been remediated and now affected over twice the number of devices. Similarly, another vulnerability that could have allowed a denial of service attack remained uncorrected. An official told us that Bonneville had not placed enough focus on the POA&M process in the past. As a result, two positions were added within the Office of Cyber Security to help officials

implement the necessary corrective actions on systems to close the POA&Ms. Absent an effective POA&M process to remediate security weaknesses in a timely manner, Bonneville's information systems will remain at a higher than necessary level of risk.

Furthermore, although Bonneville physical security and data center officials were required to review access lists quarterly and annually, we found that this control was not operating effectively. Specifically, one individual from another Federal agency had access to Bonneville's data centers for 5 years despite having never accessed the data centers. Physical security officials stated that they should have identified the person as part of the review process but could not explain why that did not occur. The Bonneville data center manager noted that he depended on others to inform him if access was no longer needed for an individual. In addition, a former data center official indicated their access had not been removed even though their position had changed. Therefore, we remain concerned that the lack of physical controls within Bonneville's data centers unnecessarily increases the risk of insider threat.

Impact and Path Forward

Without improvements to its cybersecurity program, Bonneville's systems may continue to operate at a higher than necessary risk of compromise, loss, modification, and non-availability. For instance, similar to an issue noted in our report on *The Department of Energy's July 2013 Cyber Security Breach*, the lack of remediation for certain vulnerabilities identified could have permitted an attacker or malicious user access to systems supporting business operations and other general support systems. In addition, we noted that weaknesses related to risk management and continuous monitoring could result in the authorizing official approving a system for operation even though significant deficiencies exist in the cybersecurity posture. In light of the weaknesses identified, we made several recommendations that, if fully implemented, should aid Bonneville officials in improving cybersecurity over information systems and data.

Allegations

Prior to the start of our testwork, we received two allegations concerning management of Bonneville's cybersecurity program. One allegation indicated that Bonneville officials had required nearly all teams to stop patching its information systems. The other allegation asserted that officials had not ensured that information systems contained up-to-date security controls. Based on our testing, we were unable to substantiate that Bonneville stopped patching nearly all systems. However, as indicated in our report, we found that officials had not ensured all systems were up-to-date with the latest security controls. As previously noted, scanning conducted on Bonneville's systems identified numerous unsupported software applications on network devices used to support both business and cybersecurity functions.

RECOMMENDATIONS

To improve the effectiveness of Bonneville's cybersecurity program, we recommend that the Administrator, Bonneville Power Administration:

1. Correct, through the implementation of appropriate controls, the cybersecurity weaknesses identified during our review;

2. Using the weaknesses identified in this report as well as results from our vulnerability testing, review Bonneville's remaining systems to identify and correct similar areas of concern;

3. Ensure that policies and procedures are updated and implemented consistent with Federal and internal requirements;

4. Establish an effective continuous monitoring program that includes separation of duties, implementing corrective actions to remediate POA&Ms, and strengthening data center physical security reviews; and

5. Review data center access lists to determine whether access granted is still required.

MANAGEMENT RESPONSE

Management generally concurred with the report's recommendations and indicated that corrective actions had been initiated or were planned to address the issues identified in the report. Although management fully concurred with four of five recommendations, it partially concurred with the fourth recommendation. Specifically, management did not believe that corrective actions were necessary related to separation of duties and indicated that different divisions were responsible for identifying and tracking weaknesses within the Office of Cyber Security, which sufficiently mitigated risk. To address our recommendations, management stated that it will update system security plans to ensure they are consistent with current NIST controls and control enhancements. In addition, management indicated that it will continue to identify cybersecurity weaknesses on remaining information systems through the existing security assessment process. Management also noted that policies and procedures would be updated as necessary. Furthermore, Bonneville officials commented that they will strengthen data center physical security and remove staff permissions for those no longer requiring physical access.

AUDITOR COMMENTS

Management's comments and planned corrective actions were generally responsive to our recommendations. Although management commented that it would continue to identify cybersecurity weaknesses related to Federal cybersecurity requirements through the existing security assessment process, a completion date was not identified. While we agree that management should utilize the existing security assessment process to identify weaknesses, we believe that officials should further enhance their security processes by using the results of our testing to address similar weaknesses on systems not included in our review.

Although management did not fully concur with our recommendation related to continuous monitoring and separation of duties, we continue to assert that Bonneville's Office of Cyber Security may have maintained too much authority and lacked adequate separation of duties between cybersecurity functions. While management indicated that separations existed within the Office of Cyber Security for identifying and tracking weaknesses, we remain concerned that the Office of Cyber Security was also responsible for designing, implementing, and testing controls; reviewing and approving system security plans; tracking remediation efforts; and, authorizing a number of information systems. Management's comments are included in Appendix 3.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

To determine whether Bonneville Power Administration (Bonneville) effectively implemented its cybersecurity program over its financial and administrative systems.

Scope

The audit was performed between November 2015 and August 2017 at Bonneville in Portland, Oregon. The audit included internal and external vulnerability scanning conducted by KPMG LLP on behalf of the Office of Inspector General. KPMG LLP conducted external testing of unclassified networks and systems as an outsider without any elevated privileges. KPMG LLP conducted internal scanning on both business and transmission sides 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. Test work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls. Because we were unable to separate the test results, scanning results included in this report may have information related to both business and transmission systems. The audit was conducted under Office of Inspector General project number A15TG057.

Methodology

To accomplish our objective, we:

- Reviewed applicable laws and regulations, including those pertaining to information and cybersecurity;
- Reviewed applicable standards and guidance issued by the Department of Energy;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology for the planning and management of system and information security such as Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; and National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*;
- Reviewed prior reports issued by the Office of Inspector General, the Government Accountability Office, and the Office of Enterprise Assessments;
- Held discussions with Bonneville and contractor personnel;
- Assessed controls over business network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources; and

- Contracted with KPMG LLP to conduct vulnerability scanning on Bonneville's information systems.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and Bonneville's implementation of the *GPRA Modernization Act of 2010* and determined that it had not established performance measures related to cybersecurity. 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 audit objective. However, we used computer-assisted audit tools to perform scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel. In addition, we obtained data in electronic format and used data analysis software to evaluate physical and logical access controls. We confirmed the validity of this data by cross-referencing supporting source documents and discussing potential discrepancies with Bonneville personnel.

Management waived an exit conference on August 1, 2017.

PRIOR REPORTS

- Audit Report on *The Department of Energy's Cybersecurity Risk Management Framework* (DOE-OIG-16-02, November 2015). The review determined that the Department of Energy had made progress toward implementing an unclassified cybersecurity risk management framework designed to reduce the likelihood of compromise to its information systems and data. However, we found that additional effort is needed to ensure that operating system risks are identified and systems and information are adequately secured. For example, programs and sites had not always properly categorized the risk to systems or implemented appropriate security controls. Although certain controls had been established, officials had not always thoroughly and independently assessed or monitored such controls to ensure they were effective. Further, programs and sites had not ensured that authorizing officials responsible for accepting system risk were fully aware of the risks, weaknesses, and vulnerabilities to the information systems under their purview. The weaknesses identified existed, in part, because Federal requirements for securing information systems had not been fully implemented and the Department had not established sufficient oversight and communication to support its cybersecurity risk management program. In addition, Federal officials had not provided adequate oversight to ensure effective risk management practices had been implemented. Further, Department management had not always ensured that risk tolerances were established and communicated to field elements as required to help ensure the implementation of an effective risk management program.

- Special Report on *The Department of Energy's July 2013 Cyber Security Breach* (DOE/IG-0900, December 2013). In spite of a number of early warning signs that certain personnel-related information systems were at risk, the Department had not taken action necessary to protect the personally identifiable information of a large number of its past and present employees, their dependents, and many contractors. We concluded that the July 2013 incident resulted in the exfiltration of a variety of personally identifiable information on over 104,000 individuals. Our review identified a number of technical and management issues that contributed to an environment in which this breach was possible. For example, the Department permitted direct internet access to a highly sensitive system without adequate security controls, lacked assurance that required security planning and testing activities were conducted, permitted systems to operate even though they were known to have critical and/or high-risk security vulnerabilities, and failed to assign the appropriate level of urgency to replacing end-of-life systems. We also identified numerous contributing factors related to inadequate management processes. While we did not identify a single point of failure that led to the breach, the combination of the technical and managerial problems we observed set the stage for individuals with malicious intent to access the system with what appeared to be relative ease. Without improvements to the Department's information technology and management control environment, the Department's systems containing sensitive information, including personally identifiable information, remain at a higher than necessary risk of unauthorized disclosure.

- Audit Report on *Management of Bonneville Power Administration's Information Technology Program* (DOE/IG-0861, March 2012). While Bonneville Power Administration had taken steps to address the cybersecurity concerns raised in our prior review, we identified new concerns in the areas of cybersecurity, project management, and procurement of information technology resources. Specifically, Bonneville Power Administration had not implemented controls designed to address known system vulnerabilities. In addition, operational security controls designed to protect Bonneville Power Administration's systems had not always been fully implemented. Moreover, several system development efforts suffered from cost, scope, and schedule issues, due in part to weaknesses in project planning and management. Furthermore, Bonneville Power Administration's software was not always procured in a coordinated manner, resulting in increased security risks. The issues identified were due, at least in part, to inadequate implementation of policies and procedures related to security and project management. Many of the security weaknesses identified could allow an individual with malicious intent, particularly an insider, to compromise systems and obtain unauthorized access to potentially sensitive information.

MANAGEMENT COMMENTS

Department of Energy

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

EXECUTIVE OFFICE

In reply refer to: A-7

MEMORANDUM FOR: APRIL STEPHENSON
ACTING INSPECTOR GENERAL

FROM: ELLIOT E. MAINZER
ADMINISTRATOR AND CHIEF EXECUTIVE OFFICER

SUBJECT: RESPONSE TO DRAFT AUDIT REPORT: "FOLLOWUP ON BONNEVILLE POWER ADMINISTRATION'S CYBERSECURITY PROGRAM"

The Bonneville Power Administration (Bonneville) appreciates the opportunity to provide comments on the Office of Inspector General's (OIG) draft audit report. Improved management of Bonneville's cybersecurity program is a priority for Bonneville and we agree with your recommendations as they align with the Executive Order on strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, issued May 11, 2017. This audit was initiated in November 2015. Prior to the issuance of this report, Bonneville implemented many of the actions noted in the report as part of management's ongoing commitment to continuous improvement. A summary of our response to each of the OIG recommendations is below.

Recommendation 1: *Correct, through the implementation of appropriate controls, the cybersecurity weaknesses identified during our review.*

Management Response: Concur. Prior to the issuance of this report, as part of management's ongoing commitment to continuous improvement, Bonneville implemented and enhanced controls that address the cybersecurity weaknesses in the report. These are listed below along with additional actions to continue to strengthen Bonneville's cybersecurity posture.

- Bonneville's process will continue to ensure the Bonneville Authorizing Official is fully cognizant of acceptable levels of risk prior to authorizing a system for operation. This communication is documented in the authority-to-operate letter and similar documents.
- Bonneville's access control program strengths include nearly full implementation of multifactor authentication, and integrated account management process with quarterly reviews of user account and access authorizations. This was completed June 2016.
- Bonneville will document the risk management processes that are part of the security planning process. This documentation will explain how scoping and tailoring was performed as part of the implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, titled *Security and Privacy Controls for Federal Information Systems and Organizations* for all security plans and control testing.

- Bonneville will update the six system security plans for the general support systems to ensure they are consistent with the controls and control enhancements in NIST SP 800-53, Revision 4, consistent with the risk management processes.
- Bonneville will review Federal requirements for rules of behavior and modify the initial logon screen, if necessary, since the initial logon screen communicates and requires agreement by the user to Bonneville's rules of behavior for all systems.
- Bonneville will review Federal requirements and update the contingency plans for the general support systems.

The open activities are scheduled for completion by May 2018.

Recommendation 2: *Using the weaknesses identified in this report as well as results from our vulnerability testing, review Bonneville's remaining systems to identify and correct similar areas of concern.*

Management Response: Concur. Bonneville will continue to identify cybersecurity weaknesses related to the controls in NIST 800-53, Revision 4, on the remaining systems through the existing security assessment process along with tracking through remediation in plan of action and milestones (POA&Ms). The use of POA&Ms for vulnerability tracking is in place and was improved prior to the issuance of this report. This was completed July 2016. Bonneville will continue to use the POA&Ms process to identify cybersecurity weaknesses related to the controls in NIST 800-53, Revision 4, on the remaining systems, along with tracking through remediation in POA&Ms.

Recommendation 3: *Ensure that policies and procedures are updated and implemented consistent with Federal and internal requirements.*

Management Response: Concur. Bonneville will review requirements identified in our Regulatory Compliance Program and update the policies and procedures where necessary for the following existing documents: Cyber Security Program policy, contingency planning procedures, and BPA IT Technical Architecture (BITA).

This corrective action plan is scheduled for completion by May 2018.

Recommendation 4: *Establish an effective continuous monitoring program that includes separation of duties, implementing corrective actions to remediate POA&Ms, and strengthening data center physical security reviews.*

Management Response: Partially Concur. Bonneville does not concur with the separation of duties portion of the recommendation, but does concur with the remaining elements within recommendation 4.

- Separation of Duties – do not concur: Bonneville disagrees with the recommendation to further segregate the responsibilities within the Office of Cyber Security. Bonneville's current organizational structure, with separate departments within the Office of Cyber Security responsible for identifying and tracking weaknesses, sufficiently mitigates the risk.
- Corrective Actions to Remediate POA&Ms – concur: Prior to the issuance of this report, Bonneville established a continuous monitoring program and made substantial improvements to its POA&Ms program through the addition of staff and remediation efforts focused on reducing POA&Ms with the highest risk. This was completed July 2016.
- Strengthen Data Center Physical Security – concur: Bonneville will implement controls to monitor data center access including:
  - Perform a quarterly verification review.
  - Require approval by the Bonneville Data Center Manager for all visitors.
  - Restrict visitors entering the data center to single secured doorway.
  - Require all visitors to complete an entry in the Data Center Log noting day/time of entry and exit.
  - All data center racks will be rekeyed and locked.
  - This corrective action plan will be completed by May 2018.

Recommendation 5: *Review data center access lists to determine whether access granted is still required.*

Management Response: Concur. Bonneville will review all personnel with unescorted access to our data centers, and remove permissions for staff that no longer require physical access. This corrective action plan will be completed by May 2018; with quarterly audits of the key card access list beginning in July 2017, and complete re-keying of the server racks by May 2018.

We appreciate the OIG's thorough review of our cybersecurity program and take the findings very seriously. We are committed to addressing the remaining opportunity areas. Additional information regarding our response is available as necessary and upon request.

Thank you again for the opportunity to respond to the draft audit report.

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. You may also mail comments to us:

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.