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

Audit Report

Management of Bonneville Power Administration's Information Technology Program

DOE/IG-0861 March 2012

Department of Energy
Washington, DC 20585

March 26, 2012

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Bonneville Power Administration's Information Technology Program"

INTRODUCTION AND OBJECTIVE

The Bonneville Power Administration provides about 30 percent of wholesale electric power to regional utilities that service homes, hospitals, financial institutions, commercial entities and military installations in the Pacific Northwest. Bonneville makes extensive use of various information systems in its daily operations, including electricity transmission systems, systems that enable the marketing and transferring of electrical power, as well as administrative and financial systems. Should any of these information systems be compromised or otherwise rendered inoperable, the impact on Bonneville's customers could be significant.

Prior reviews have identified weaknesses related to Bonneville's information technology (IT) program. For instance, our report on *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008) identified risk management weaknesses related to Bonneville's Federal requirement to certify and accredit its information systems for operation, a problem that could adversely impact the security of critical systems and the data contained therein. In this light, we initiated this audit to determine whether Bonneville effectively and efficiently implemented its IT program.

RESULTS OF AUDIT

Bonneville had taken steps to address the cyber security concerns raised in our prior review. For instance, officials had performed detailed assessments of security controls on various general support systems. However, our current review identified new concerns in the areas of cyber security, project management and procurement of IT resources:

- Bonneville had not implemented controls designed to address known system vulnerabilities. Specifically, technical vulnerability scanning conducted on nine applications used to support business functions such as financial management, human resources and security management identified a significant number of high-risk weaknesses in the areas of access controls, patch management and validation of user input;

- Operational security controls designed to protect Bonneville's systems had not always been fully implemented. For instance, testing of five systems identified issues with configuration management, least privilege, and contingency and security planning;

- Several system development efforts suffered from cost, scope and schedule issues, due in part to weaknesses in project planning and management. For example, we noted that one project was completed more than 16 months behind schedule and approximately $7 million over the initial budget at the time the development effort was approved, even though the scope of the effort had been significantly reduced; and,

- Bonneville's IT software was not always procured in a coordinated manner, resulting in increased security risks. Specifically, we identified a lack of adherence to approved software listings for procurements.

The issues identified were due, at least in part, to inadequate implementation of policies and procedures related to security and project management. For instance, we found that responsible officials were not taking action to remediate or mitigate known system security vulnerabilities, as required. We also determined that inadequate planning of resource requirements prevented Bonneville from effectively managing its IT program. Specifically, Bonneville had not allocated sufficient resources to cyber security and system development efforts to help ensure that effective management practices were implemented. Furthermore, we found that Bonneville's Office of the Chief Information Officer did not have authority over the entire IT program, including certain cyber security and procurement functions.

Without improvements, Bonneville's systems and information may be exposed to a higher than necessary level of risk of compromise, loss, modification and nonavailability. Many of the security weaknesses we identified could allow an individual with malicious intent, particularly an insider, to compromise systems and obtain unauthorized access to potentially sensitive information. Utilizing unapproved software can result in additional costs and a less secure computing environment through the introduction of vulnerabilities in unsupported software.

In addition, Bonneville may continue to experience problems related to project management and spend more than necessary on IT resources. While we did not identify a direct correlation between the reported project slippages and a failure in management's decision-making processes, the changes to scope and schedule did impact management's ability to effectively manage its limited resources and may have affected its ability to initiate other projects.

Prior to initiating our audit, we received several allegations regarding IT management improprieties at Bonneville. Through our testing, we were able to substantiate certain aspects of the allegations as they related to security planning. Our findings in that area have been incorporated into our results and are discussed with more specificity in the body of our report. The remainder of the allegations, described in Appendix 1, were not substantiated.

Due to security considerations, details regarding the specific systems for which vulnerabilities were identified have been omitted from this report. Management officials, however, were provided detailed information regarding the issues we identified and had initiated certain corrective actions. In addition, officials were implementing compensating security controls to help limit access to potentially sensitive data. While these are positive efforts, additional steps are necessary to reduce risk to information systems and improve project management and acquisition practices. As such, we made several recommendations designed to address the issues outlined in our report. These recommendations, generally considered to be best practices in the Federal IT environment, should, if fully implemented, enhance management of Bonneville's IT program.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that corrective action would be taken. Management commented that, though it believed it had historically resourced projects adequately, it was committed to improving demand planning capability. Further, while management stated that the positioning and established authority of Bonneville's Chief Information Officer was appropriate, it commented that it was working to extend authority over the entire IT program.

Management disagreed with several of the conclusions in the report, particularly in the area of project management. For example, management commented that over 80 percent of completed IT projects were accomplished within schedule, budget and scope. We found, however, that management's re-baselining of projects resulted in projects being reported as completed within set parameters even though these projects may have significantly exceeded initial cost, scope and schedule estimates. As a result, the importance of effective project planning was significantly devalued, and systems did not always provide the desired capabilities when expected. As appropriate, we modified our report in response to management's comments. Bonneville's comments and our rebuttals to management's disagreements are summarized and more fully discussed in the body of our report. Management's comments are included in Appendix 4.

Attachment

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

REPORT ON MANAGEMENT OF BONNEVILLE POWER ADMINISTRATION'S INFORMATION TECHNOLOGY PROGRAM

TABLE OF CONTENTS

Cyber Security, Project Management and Procurement

Appendices

MANAGEMENT OF BONNEVILLE POWER ADMINSTRATION'S INFORMATION TECHNOLOGY PROGRAM

Program Improvement

The Bonneville Power Administration (Bonneville) had taken positive steps to strengthen its cyber security program. In particular, we noted that corrective actions had been taken to resolve weaknesses identified during our audit of *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008). Specifically, Bonneville had:

- Enhanced management attention over the cyber security program by appointing its Chief Operating Officer as the official responsible for accepting risk-based decisions and authorizing systems for operation;

- Educated information system owners about their responsibilities for managing cyber security risks related to information systems and hired personnel in its cyber security group to enhance the group's skill set; and,

- Developed various system security plans and initiated efforts to verify that necessary security controls were sufficiently tested for each system through security assessments and continuous monitoring activities.

Bonneville also enhanced management and oversight of its information technology (IT) projects through the establishment of the Project Management Office (PMO). In addition, the establishment of the Agency Prioritization Steering Committee provided senior-level approval and oversight of planned and ongoing projects.

Cyber Security, Project Management and Procurement

Our review of Bonneville's IT program identified several areas of concern related to cyber security, project management and procurement of IT resources. In particular, required security controls designed to protect Bonneville's systems had not always been implemented. Technical vulnerability testing and reviews of process-oriented security controls identified various weaknesses that increased the risk to those systems. In addition, project management weaknesses contributed to significant increases in cost, scope and schedule during the life cycle of various IT projects. Furthermore, software was not always acquired in a coordinated manner and did not always conform to established standards.

Vulnerability Management

Technical testing of certain Bonneville information systems identified significant weaknesses in the areas of access controls, patch management and validation of user input. We performed vulnerability scanning on nine applications used to support Bonneville's business functions related to financial management, human resources and security management. Due to concerns from Bonneville officials, testing did not include systems operated by Bonneville's Transmission Operations organization. We found:

- Systems had not always been configured to prevent unauthorized access. For instance, our testing identified 11 servers that were configured with weak passwords, an issue that could have allowed a knowledgeable attacker to obtain complete access to the system. In addition, four servers were configured to permit all remote users to access and modify shared files – some of which contained potentially sensitive information. Officials commented that they had implemented certain controls to address the weaknesses identified;

- Patches to address known vulnerabilities had not been applied to software in a timely manner. Our testing identified more than 400 vulnerabilities that were designated as high-risk in the National Vulnerability Database, which is sponsored by the Department of Homeland Security. The vulnerabilities involved weaknesses attributable to seven commercial off-the-shelf (COTS) products utilized by Bonneville that had not been patched when security updates became available. Of those vulnerabilities, 34 percent were more than 18 months old, including 33 that were associated with known exploits that had been identified in 2007 or earlier. The vulnerabilities identified were known to allow, among other things, unauthorized access and introduction of malicious code. In response to our report, management disagreed with the total number of unique vulnerabilities but stated that it had taken action to remediate the identified weaknesses. In addition, we identified three servers that were running software that was no longer supported by the manufacturer, a condition which increased the risk of exploit on those servers as patches were no longer being issued when vulnerabilities were identified. Bonneville told us that it was aware of the outdated software issue and that efforts were underway prior to the audit to migrate the servers to a

current software version. We noted, however, that a plan to do so had not been completed by the end of our fieldwork; and,

- Systems reviewed did not always validate user inputs to ensure that the data was in the proper format and met expected criteria. For example, certain servers did not ensure that valid information was received from the user, an action or control designed to prevent attackers from crafting malicious code designed to damage systems or permit the theft of sensitive data.

When informed of the results of our testing, management indicated that actions were being taken to correct the issues we found. However, until these vulnerabilities are fully remediated and controls are in place to promptly ensure that software is updated in an expeditious manner, Bonneville's systems remain at a higher than necessary level of risk of exploit by malicious individuals.

System Security Controls

Our testing also revealed a number of issues related to process-oriented security controls for five systems. These weaknesses could increase the risk of compromise to Bonneville's information resources. In particular, we noted weaknesses related to implementation of standard security configurations, application of least privilege principles, contingency planning and system security planning. Specifically:

- Bonneville had made only limited use of standard security baselines designed to ensure that operating systems were secured. Specifically, even though the U.S. Government Configuration Baseline initiative, formerly the Federal Desktop Core Configuration initiative, required that standard configurations be established for all operating systems used by Federal agencies, we found that Bonneville had developed and implemented standard configurations for only two of its four server operating systems. In commenting on our report, management stated that it anticipated developing and implementing standard configurations for the remaining operating systems in Fiscal Year (FY) 2012. We also identified more than 550 instances of individuals that had local administrative privileges on their desktops or laptops, authority that would have permitted users to make unauthorized security-related changes to their computers;

- The principle of least privilege was not applied across Bonneville's IT environment. Specifically, we identified 12 instances where regular users had been assigned administrative privileges to servers based on group membership. Eleven of the 12 instances included privileged access given to individuals having no need for such permissions, including 3 individuals whose job responsibilities required no access to the system. By implementing least privilege, officials would have provided only the access necessary for individuals to perform tasks within their span of responsibility;

- Contingency plans had not always been developed or tested on the systems reviewed. Specifically, only two of six systems had contingency plans that were documented and tested for effectiveness. Three system owners had not developed contingency plans for their systems because they stated they were waiting for representatives from Bonneville's Office of Business Continuity to facilitate the design and drafting of their systems' contingency plans. As required by the National Institute of Standards and Technology (NIST), information system owners should develop, test and revise contingency plans on a regular basis as part of maintaining a system's operation; and,

- In one particular instance, we noted various weaknesses related to security planning for a major system. Specifically, the system, which was hosted by a contractor in Canada, had not been categorized to determine at what level the confidentiality, integrity and availability of the system and its information should be protected. In addition, security planning documentation did not detail NIST-compliant controls and did not assign responsibility for the system to any Federal official. Further, although in use, the system had not received authority to operate and only recently had a system security plan drafted. We also noted that even though Bonneville's security functions did not agree with the decision to house the system on servers residing in a foreign country, the system owners placed it into operation. Bonneville subsequently experienced two instances wherein numerous documents marked as "Official Use Only" were inappropriately housed on the system at the contractor's location, thereby increasing the risk of unauthorized access. Our review of this system was initiated to resolve allegations received through the

Office of Inspector General's Hotline. Based on the issues noted above, we were able to substantiate the information in the complaint. To its credit, management took a number of actions to implement controls designed to prevent further similar occurrences.

Project Management

We found that multiple projects managed by Bonneville's PMO suffered from cost, scope and schedule issues during the projects' life cycles. During our detailed review of selected projects managed by the PMO, we noted various issues related to project planning and management that likely contributed to the observed issues.

In particular, we identified project planning issues with the Transmission Asset System (TAS) and noted that the system underwent significant modifications to its cost, scope and schedule after the business case was initially approved. Cost estimates for project completion had been modified at least twice and were considerably higher than originally planned. While the TAS project was approved for development in 2009 at an estimated cost of $4.5 million, the cost to complete the project rose to approximately $7.4 million a short time later when it entered the execution phase. Subsequently, the estimated cost of the project increased again to more than $12 million even though its functionality had been significantly reduced. Officials told us that preliminary planning costs were only rough estimates and that the planned cost was actually $8.3 million. We found, however, that the decision to proceed with the project was based, in part, on the original estimate of $4.5 million. Officials reported that the project was ultimately completed for $11.5 million in July 2011, 16 months later than originally planned.

In addition to widely varying cost estimates for the TAS project, we also found that actions undertaken early in the project's implementation did not adequately consider or fully define requirements. We noted that in at least two instances, elements related to scope such as whether the project met user needs and system or resource requirements were not adequately considered. After a major software application was procured, the project team determined that the application may not work with two of the groups planning to utilize the project. As a result of the incomplete analysis prior to acquiring the software, the project's scope was reduced by two-thirds to account for the groups that could not utilize the software purchased. In addition, IT equipment necessary to support the project was not adequately tested to

ensure compatibility with Bonneville's approved software suite. Specifically, encryption software was not fully tested on certain types of computers prior to procurement, and as a result, the software was found to be incompatible and will need to be replaced. In preliminary comments to our draft report, officials stated that the lack of encryption on those devices did not increase the risk since information had not been previously encrypted.

In addition, Bonneville officials reported that the Governance, Risk and Compliance (GRC) Resolver project also exceeded its estimated cost and schedule even though the initial scope was reduced. Although officials initially documented the need for the project, we found that planning documentation was high-level and did not adequately consider activities related to cost-benefit analyses, project schedule or user requirements. For instance, while originally intended for use by multiple program offices at Bonneville, the scope of the project was reduced so that only one office had access to and was utilizing the system. The remainder of the project's scope is now proposed to be completed as separate projects at additional cost. Bonneville was unable to provide documentation to support various phases of the project life cycle, including both planning and execution. Even with a decreased scope, the project exceeded its initial budget by almost $160,000.

Similar to issues related to projects managed by the PMO, we also identified problems with the Dispatch Logging System managed by the Transmission Operations organization. Specifically, we found that over the life of the project, the budget had increased by approximately $650,000 to $3.2 million. In addition, while initially scheduled for completion in May 2005, the project was not completed until late in 2010 – approximately 5 years later. As with the other projects reviewed, the Dispatch Logging System's scope had been modified to include functions that were not identified or included as part of the original project planning process. Specifically, initial planning documentation did not include relevant information related to all components of the project, training costs and detailed schedule with dates, milestones and resource needs.

Software Standards

Bonneville had not always adhered to its approved standards when procuring software. For example, Bonneville had purchased several types of software over a 3-year period that had not been properly tested by cyber security and included on an approved software list to ensure that it would not conflict with Bonneville's operating environment. Our analysis determined that about 50

percent of software purchases by Transmission Operations were for software packages not included on the approved listing, compared to only about 7 percent for the rest of Bonneville. Utilizing unapproved software can result in additional costs and a less secure computing environment through the introduction of vulnerabilities in unsupported software.

Policies and Procedures, and Organization

The issues identified were due, in part, to inadequate implementation of policies and procedures for security, project management and acquisition. We also found that Bonneville had not allocated sufficient resources to effectively manage its IT program. Furthermore, Bonneville's Office of the Chief Information Officer (OCIO) did not have authority over the entire IT program, including certain cyber security and procurement functions.

Security Policy and Procedures

Bonneville officials had not ensured that policies and procedures related to cyber security were effectively implemented. For instance, officials had not ensured that procedures for limiting administrative privileges on user accounts were effectively implemented. In addition, although the Bonneville patch management policy required that system owners and administrators remediate or mitigate vulnerabilities, we found that this was not being done for many of the systems reviewed. Contrary to the policy, system owners we spoke with commented that they did not believe patching systems was part of their responsibilities. Similarly, various system owners believed that they were not responsible for implementing other security controls such as access controls, contingency planning and security planning. Representatives for one system commented that the project team and outsourced services provider were responsible for knowing the protection requirements for their system's information instead of the information and system owners. In another case, multiple system owners commented that the responsibility for contingency planning efforts rested with Bonneville's Office of Business Continuity. However, NIST and Bonneville's Program Cyber Security Plan noted that this responsibility lay with system and information owners. Furthermore, we found that the lack of coordination between system owners and cyber security personnel resulted in an increased risk of unauthorized access to potentially sensitive information for one system reviewed. These problems are similar to those identified in our prior report on *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008).

Project Management and Procurement Policy and Procedures

Several of the project management and acquisition issues we identified were also the result of ineffective development and/or implementation of requirements designed to ensure adequate project planning. Bonneville's System Development Life Cycle (SDLC) documented specific project phases but did not require that projects be well-defined prior to completion of the planning phase. Instead, detailed designs and implementation plans were required to be completed during the execution phase. As a result, elements such as cost, schedule and scope did not need to be fully defined until after a project was approved and execution was underway. The ability to begin the execution phase without having fully determined a project's expected cost, schedule and scope directly contributed to many of the issues we identified. Documented project management policies and procedures also did not detail actions to be taken to ensure that similar slippages did not occur on future projects.

While management provided oversight related to project changes, the project planning process was not always effective. Specifically, project managers and their teams did not always adhere to SDLC planning requirements and made significant changes to project scope during project execution. Specifically, as noted previously, the TAS project experienced significant scope reductions during its implementation phase because officials acquired software that did not support the needs of the entire project. In particular, officials eliminated certain components of the project that could not be supported by the software purchased – deciding instead to focus only on a piece of the originally planned project. In addition, the cost of the project nearly tripled over initial estimates because project managers did not effectively budget for expected costs. Although management was aware of the proposed changes, a more effective planning process may have reduced the need for such modifications and allowed Bonneville to more effectively budget for costs. Similarly, officials reduced the scope of the GRC Resolver project because they had not adequately planned the project and exhausted funding prior to completion.

In addition, the SDLC did not fully detail the timing of required coordination with cyber security during the project management process. This lack of clarity contributed to several of the problems we noted above, including issues with untested software on the TAS project. In comments on our draft report, management stated that the SDLC had recently been updated to address many of the issues we identified. Based on our review of the updated SDLC, if

fully implemented and utilized as intended, many of the problems identified related to project management could be avoided in the future.

We also identified weaknesses related to implementation of Bonneville's procurement policies. Specifically, we noted instances where the Supply Chain organization purchased software that did not conform to organizational standards even though the Bonneville Purchasing Operation Procedures stated that the buying decision for requests rested with the Supply Chain. Supply Chain representatives stated that they sometimes questioned non-standard requests but did not believe they had the expertise to challenge the requests or were overruled by the requesting organization. While we acknowledge that exceptions to standards are necessary at times, we noted that the lack of rigor in the process minimized the usefulness of the standards.

Resource Planning and IT Organizational Placement

We found that resource allocation decisions at Bonneville likely contributed to some of the issues we identified during our audit. In addition, the organizational structure of Bonneville did not fully support an effective program. For instance, issues related to project management were impacted by resource allocation strategies. In certain instances, staff at Bonneville told us that they lacked adequate resources to develop projects and perform duties related to ongoing maintenance and operations. For example, programmers for the Dispatch Logging System were frequently reassigned to other projects, resulting in missed timelines and higher than necessary costs. Similarly, the GRC Resolver project manager told us about having to work on three projects and not having have sufficient time to spend on managing the project effectively. We also noted that the Network Reconstruction project was suspended for approximately two years due to a lack of server team resources.

We also noted that lines of authority in its IT program adversely affected Bonneville's cyber security posture. For example, although the cyber security organization within the OCIO performed system control testing and periodic vulnerability scanning, it lacked the ability to ensure other organizations remediated weaknesses identified as part of testing, significantly limiting the value of the testing. In addition, the OCIO did not have purview over IT operations and procurements that were part of Transmission Operations. These practices were contrary to

NIST guidance which states that the Chief Information Officer (CIO) is responsible for developing, maintaining and facilitating the implementation of a sound IT program.

Secure and Cost-Effective Information Technology Management

Without improvements to its IT program, Bonneville's systems and information may be exposed to a higher than necessary level of risk of compromise, loss, modification and nonavailability. In addition, Bonneville may continue to experience problems related to project management and spend more than necessary on IT resources. While we did not identify a direct correlation between the reported project slippages and a failure in management's decision-making processes, the changes did deprive management of the ability to effectively manage its limited resources. Further, it may impact the ability to initiate other projects. Many of the security weaknesses we identified could allow an individual with malicious intent, particularly an insider, to compromise systems and obtain unauthorized access to potentially sensitive information. The number of vulnerabilities we identified was especially troubling given the nature and age of the weaknesses and the lack of an effective, risk-based process for addressing them. During preliminary discussions of our report, Bonneville informed us that it had initiated certain cyber security corrective actions.

Similarly, without improved planning and attention to established requirements, ongoing and planned IT projects may continue to experience problems meeting cost and schedule milestones, ultimately impacting Bonneville's mission. Furthermore, given current procurement trends, Bonneville will continue to encounter risks to its systems by introducing unapproved software into the operating environment.

RECOMMENDATIONS

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

1. Correct, through the implementation of appropriate controls, the cyber security weaknesses identified in this report;

2. Ensure that policies and procedures are developed, as appropriate, and are adequately implemented to address weaknesses related to cyber security, project management and IT procurement;

3. Implement effective resource planning and allocation to meet IT program needs; and,

4. Re-evaluate the authority of Bonneville's OCIO within the organization and take action as necessary to ensure sufficient visibility, accountability and oversight of the IT program.

MANAGEMENT REACTION AND AUDITOR COMMENTS

Management concurred with the report's recommendations and indicated that corrective actions would be taken. Management commented that it was committed to improving the IT program accordingly and believed that it had made significant improvements in the cyber security and project management programs over recent years. In addition, management expressed concern that the report did not completely reflect the effectiveness and efficiencies of Bonneville's IT program.

Management commented that, though it believed it had historically resourced projects adequately, it was committed to improving demand planning capability. Further, while management stated that the positioning and established authority of Bonneville's CIO was appropriate, it commented that it was working to extend the OCIO's authority over the IT program. We found that, while the organizational placement of Bonneville's CIO may have been appropriate, the OCIO did not have authority over the entire IT program, including certain cyber security and procurement functions. As noted in our report, the OCIO was responsible for conducting vulnerability testing of Bonneville's information systems, but did not have the authority to remediate weaknesses, thereby limiting the value of the testing.

We have addressed management's comments in more detail in the following paragraphs and made technical changes to the report, as appropriate. Management comments are included in their entirety in Appendix 4.

Cyber Security

Management agreed that it needs a more effective patch management program, but stated that the number of high-risk vulnerabilities we identified was duplicative and that the actual number of vulnerabilities was lower than reported. Management also indicated that it was aware of the weaknesses we discovered and had initiated action to remediate the identified vulnerabilities. While management's planned corrective actions are commendable, we disagree with its assertion that the number of vulnerabilities identified was overstated. Specifically, the 400 vulnerabilities referred to in the report were related to unique high-risk vulnerabilities identified during internal vulnerability scanning. In

addition, at the time of our test work, management indicated that it was unaware of several specific vulnerabilities that we identified. We provided management with support for the number of vulnerabilities identified, but did not evaluate how many were remediated subsequent to our test work. Furthermore, although management stated that its passwords met industry standards, we found at least one administrative account with a default password.

Management stated that it had an effort underway to develop contingency plans for information systems, as appropriate. In particular, officials noted that although formal contingency plans did not exist for certain systems, processes were in place that had been tested for contingency planning purposes. Management also commented that a contingency plan was not required for one of the systems reviewed because it was hosted by an offsite vendor. However, Bonneville was unable to provide us with documentation to demonstrate that it had taken steps to obtain assurance over the vendor's contingency planning processes.

Project Management

Management believed that system development efforts were effective and stated that over 80 percent of completed IT projects were accomplished within schedule, budget and scope. Although we agree that certain measures implemented by Bonneville may have enhanced effectiveness such as the establishment of the PMO, our report demonstrated that various weaknesses continued to exist. Based on our review of documentation provided by Bonneville and interviews with project officials, we disagree with management's assertion that it completed 80 percent of IT projects within schedule, budget and scope. In particular, management's re-baselining of projects resulted in projects being reported as completed within set parameters even though these projects may have significantly exceeded initial cost, scope and schedule estimates. As a result, the importance of effective project planning was significantly devalued, and systems did not always provide the desired capabilities when expected.

Management agreed that the TAS project underwent significant changes to cost, scope and schedule, but stated that the cost figures cited in our report were misleading. Specifically, management commented that while $4.5 million was an initial cost projection, the approved cost after vendor selection and completion of planning activities was $8.3 million. Management stated that the TAS project was successfully delivered according to its approved business case. Management also commented that the areas of

scope removed from the TAS project were still being pursued by the organization. We agree that while the TAS project was delivered, it significantly exceeded the estimated cost and schedule. As noted in our report, the TAS project experienced several re-baselining efforts that culminated in the project being completed at nearly three times the cost estimate used to approve the development effort. Even though the costs increased, the scope of the project was significantly reduced. Although management commented that the scope removed from the project was still being pursued, our interviews with members of the project team indicated that the scope reduction was necessary due to a lack of full comprehension of project requirements during the planning process.

Management commented that the GRC Resolver project's scope was reduced in an effort to support regulatory compliance that was deemed to be the highest priority aspect of the project. In addition, management stated that the Dispatch Logging System's delay was due to a reallocation of resources and that changes to scope were approved by project sponsors. We agree that project changes described in management's comments were approved by executive sponsors and formal oversight committees. However, as with the TAS project, our concerns are centered around the lack of initial project planning that contributed to increased costs and timelines, and reduced project scope. Best practices for software development issued by the Carnegie Mellon Management Institute suggest that firm budgets and schedules be developed during project planning to enhance the ability of a project being completed on time and within budget.

Management disputed our assertion that Bonneville had inadequate resources to manage its IT program. We found, however, that the GRC Resolver project suffered from a lack of continuous project management. For instance, we noted that the project had at least three separate project managers and that information supporting the project was not always passed from one manager to the next. Ultimately, the project was completed approximately five years behind schedule.

Management disagreed with our assertion that documented project management policies and procedures did not detail actions to be taken to ensure that schedule slippages did not occur on future projects. Although management cited that the Project Manager's Handbook stated that managers should avoid having to process IT change orders during the execution phase of a project, we found that the ability to begin the execution phase without having fully

determined a project's expected cost, schedule and scope directly contributed to many of the issues we identified. Further, policies and procedures did not require specific actions to be taken as a result of lessons learned during projects that exceeded their milestones.

Management disagreed with our statement that Bonneville did not always adhere to SDLC planning requirements and made significant changes to project scope during project execution. We agree that changes to project scope, schedule and costs occur during project life cycles; however, the extent of these changes at Bonneville is the reason for our concern. We believe that if projects were better planned early in the life cycles, the need to initiate significant re-baselining efforts such as those identified during our review could be alleviated, and projects may be completed more timely and closer to initial budgets.

Management commented that the SDLC required that detailed activities such as development of cost estimates and schedules occur prior to project execution getting underway. Management also stated that the purpose of the planning phase outlined in the SDLC was to perform sufficient planning and analysis to develop the business case, and to support a build versus buy decision. In addition, management commented that the SDLC had been updated to better align planning and execution activities. We agree with management's statements regarding the timing of cost estimate and schedule development. However, as previously mentioned, best practices suggest that these activities should take place before a project exits the planning phase. We continue to believe that ensuring projects are properly planned prior to execution would relieve some of the issues we identified with Bonneville's schedule slippages. Bonneville's recently updated SDLC appears to address this issue, and we are hopeful that full implementation of this document will improve its project management process.

OTHER MATTERS

Prior to our review, the Office of Inspector General received a hotline complaint that alleged conflicts of interest between the Bonneville Power Administration (Bonneville) and a consulting firm used to provide supplemental labor in its project management office. The complaint asserted that the firm provided project managers and staff for all major information technology projects at Bonneville and stated that Bonneville had utilized the firm's services to perform an assessment of the Data Center Modernization (DCM) project. Upon completion of the assessment, the project's scope and staffing were modified to address the firm's recommendations.

To address the complaint, we performed steps to evaluate management of the DCM project. In particular, we reviewed and analyzed documentation related to the DCM project, including a presentation given to Bonneville's Agency Prioritization Steering Committee detailing the results of the assessment, and interviewed Bonneville officials regarding project management practices.

We were unable to substantiate the allegation of a conflict of interest between Bonneville and its supplemental labor contractor. Specifically, while the contractor was asked to perform a review of the project's progress and status, it was neither intended nor required to be an independent assessment. Rather, it was an internal review intended to inform Bonneville's upper management of the project's status for the purposes of further funding and prioritization. We also evaluated project management activities related to DCM and did not identify any significant weaknesses.

Appendix 2

OBJECTIVE

To determine whether the Bonneville Power Administration (Bonneville) effectively and efficiently implemented its information technology (IT) program.

SCOPE

The audit was performed between October 2010 and March 2012, at Bonneville Headquarters in Portland, Oregon. The audit was limited to a review of Bonneville's cyber security, IT project management and procurement programs. Vulnerability scanning was performed on selected business systems at Bonneville. However, we did not conduct vulnerability scanning on systems managed by Bonneville's Transmission Operations organization.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and regulations, including those pertaining to cyber security, IT project management and IT procurement;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology;
- Reviewed prior reports issued by the Office of Inspector General and the Department of Energy's Office of Health, Safety and Security;
- Obtained documentation from, and held discussions with, officials from Bonneville's Office of the Chief Information Officer, cyber security, project management, procurement, and Transmission Operations organizations; and,
- Performed internal and external vulnerability scanning to determine vulnerabilities related to specific systems within Bonneville.

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 objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the objective. In particular, we assessed Bonneville's implementation of the *Government Performance and Results Act of 1993* and determined that it had not established performance measures for cyber security, project management or procurement.

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 conducted an assessment of computer-processed data relevant to our audit objective and found it to be sufficiently reliable.

An exit conference was held with Bonneville officials on March 14, 2012.

PRIOR REPORTS

- 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 or DOE). 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 (FY) 2012 includes cyber security, and contract and financial assistance award management.

- Audit Report on *Cyber Security Risk Management Practices at the Bonneville Power Administration* (DOE/IG-0807, December 2008). The audit identified risk management weaknesses related to the certification and accreditation of Bonneville Power Administration's (Bonneville) critical information systems. In particular, Bonneville had not always appropriately identified and addressed potential risks to critical systems and data, to include systems controlling electricity transmission; developed adequate security plans for each of the four systems we reviewed; ensured that physical and cyber security controls were tested and operating as intended; and, developed corrective action plans necessary to resolve weaknesses in a number of important control areas. Problems with the certification of these systems – some of which are integral to controlling electrical transmission to western portions of the United States – were attributable to Bonneville's failure to fully adopt a risk-based approach for implementing security controls that satisfied Federal requirements. In addition, Bonneville had not adequately emphasized the importance of a robust cyber security program through involvement of system and information owners.

- Audit Report on *Facility Contractor Acquisition and Management of Information Technology Hardware* (DOE/IG-0768, June 2007). Certain Department facility contractors had not adequately managed the acquisition and control of information technology (IT) hardware. A number of contractors had not consistently taken advantage of opportunities to reduce acquisition and support costs, addressed security concerns related to certain aging systems or ensured that accountability was maintained over sensitive computers and devices. In particular, we observed that five of the seven sites we reviewed had not developed or fully implemented hardware specifications and brand standards for computers and related peripherals, directly contributing to unnecessary expenditures of at least $4.7 million over a 3-year period. Widely divergent hardware replacement cycles contributed to problems ranging from supporting outdated computers to replacing equipment before the end of its service life. Sites had not always taken advantage of opportunities to achieve volume purchase discounts. Several sites did not track certain sensitive IT equipment, including laptop computers and personal digital assistants. These problems occurred because the Department had not developed a coordinated approach to IT hardware acquisition, management and control.

- Audit Report on *Information System Development Practices at the Bonneville and Western Area Power Administrations* (DOE/IG-0586, February 2003). The audit found that Bonneville and Western Area Power Administration (Western) information system development activities were not always consistent with Federal requirements or guidance. Specifically, we found significant problems with 9 of the 11 major projects included in our review. In addition, neither Bonneville nor Western was able to assess the benefits versus resource expenditures for development efforts because project managers did not consistently account for all relevant project costs. We identified a number of areas in which system development activities could be improved. Consequently, management often lacked information necessary to properly evaluate investment decisions and did not take sufficient action to prevent or ameliorate significant implementation delays and project cost overruns totaling over $11 million.

MANAGEMENT COMMENTS

Department of Energy

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

EXECUTIVE OFFICE

February 21, 2012

In reply refer to: NJ-3

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

FROM: STEPHEN J. WRIGHT
ADMINISTRATOR AND CHIEF EXECUTIVE OFFICER

SUBJECT: RESPONSE TO DRAFT AUDIT REPORT ON MANAGEMENT OF BONNEVILLE POWER ADMINISTRATION'S INFORMATION TECHNOLOGY PROGRAM

The Bonneville Power Administration (Bonneville) appreciates the opportunity to comment on the draft final report of the subject audit. While we agree in part with the Office of Inspector General's (OIG) recommendations and are committed to actions to improve our program accordingly, we take issue with some specific assertions made in the report. We believe the report does not reflect the adequacy of some of our processes and sometimes draws conclusions that may mislead readers about the effectiveness of our Information Technology Program (IT). Bonneville plays a vital role in the economy of the Pacific Northwest, and therefore, it is important that our customers and other stakeholders understand the importance Bonneville places on continuously improving our IT program to ensure it is secure, effective, and cost-efficient.

The OIG's draft report cited a number of high-risk weaknesses found through vulnerability scanning, conducted on nine applications. We were previously aware of these weaknesses, through our own vulnerability scanning program, and have initiatives underway to improve our security posture in these areas. Specifically, we are implementing a more robust patch management program, with special attention given to the challenges of patching legacy applications.

The OIG also cited inadequate planning of resource requirements and stated that management had not allocated sufficient resources to system development efforts. We, however, believe that the fact we have completed over 80% of our IT projects for FY2010 and FY2011 within scope, on schedule, and within budget, is sufficient evidence that our development efforts have been adequately resourced. Nonetheless, as an element of our continuous improvement efforts we will implement a new Demand Planning System, which will improve our ability to allocate labor resources across all of the projects in our project portfolio by the end of the fiscal year.

Bonneville is fully committed to continuous improvement in IT, as evidenced by improvements we have made in our governance of project development activities and our establishment of a Project Management Office (PMO). Projects managed by the PMO receive funding approval and oversight from the Agency Prioritization Steering Committee (APSC), an agency-wide committee of senior-

Bonneville is fully committed to continuous improvement in IT, as evidenced by improvements we have made in our governance of project development activities and our establishment of a Project Management Office (PMO). Projects managed by the PMO receive funding approval and oversight from the Agency Prioritization Steering Committee (APSC), an agency-wide committee of senior-level management. Bonneville's IT PMO processes are governed by a formal Systems Life Cycle (SLC) methodology covering all phases of an IT project from inception through implementation and post-audit.

Bonneville has also made significant progress in maturing its Cyber Security and Information Assurance functions. These activities have resulted in the establishment of System Security Plans (SSP), the identification of Information System Owner (ISO) and Information Owner (IO) roles for each system, a rigorous Security Assessment Review (SAR) process, and an Authority to Operate (ATO) process that engages Bonneville's Chief Operating Officer in the risk decision to implement new automation solutions. The omission of these IT maturity achievements gives the uninformed reader the impression these important processes are not in place.

While we appreciate the value of external audits to assess our improvement efforts, we are concerned that this assessment does not completely reflect the effectiveness and efficiencies of Bonneville's IT program. We address specific OIG findings and further describe the status of related efforts in our appendix, available at http://www.bpa.gov/corporate/pubs/audits/ .

Our plan to address the draft report's recommendations will be adopted within 180 days of the OIG final report. Specifically, as to recommendation #1, we concur and will layout our plan to improve our overall cyber security posture. As to recommendation #2, we concur and will develop policies and procedures as an element of our continuous improvement initiatives. As to recommendation #3, though we believe we have historically resourced our projects adequately, we are committed to improving our demand planning capability and to that extent, concur with this recommendation. Finally, as to recommendation #4, we concur in part, as we believe the positioning and established authority of the CIO is appropriate but acknowledge there are opportunities to further exercise that authority through extension of CIO governance in the Transmission Services area.

Thank you for this opportunity to address the draft report. If you have further questions, please contact Larry Buttress, Chief Information Officer, at (503) 230-3690.

cc:
Director, Office of Risk Management and Financial Policy, CF-50
Assistant Director, Office of Risk Management and Financial Policy, CF-50
Team Leader, Office of Risk Management and Financial Policy, CF-50
Audit Resolution Specialist, Office of Risk Management and Financial Policy, CF-50
Audit Liaison, Office of the Chief Information Officer, IM-10

IG Report No. DOE/IG-0861

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 they are 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 which 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.