U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Cyber Security Risk Management Practices at the Bonneville Power Administration

DOE/IG-0807

December 2008

Department of Energy
Washington, DC 20585

December 9, 2008

MEMORANDUM FOR THE SECRETARY

FROM: Greg Friedman
Gregory H. Friedman
Inspector General

SUBJECT: Audit Report on "Cyber Security Risk Management Practices at the Bonneville Power Administration"

BACKGROUND

The Bonneville Power Administration (Bonneville) provides electrical power to millions of customers in eight states in the Pacific Northwest. To support this critical function, Bonneville makes extensive use of a number of information systems to conduct various activities, including financial management, operation of extensive electricity transmission systems, and marketing and transferring wholesale electrical power. Some of Bonneville's most sensitive systems are used to help control the flow of electricity to the power grid. Should any of these control systems be rendered inoperable for an extended period, Bonneville's customer base could be adversely impacted.

To help identify and manage risk, all Federal entities are required to certify and accredit (C&A) their information systems. The C&A process is a recognized, methodical process designed to ensure that information systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The C&A process includes specific steps to recognize and address risks, determine whether system security controls are in place and operating effectively, and ensure that changes to a system are adequately tested and approved. In light of the growing threat to security over information systems supporting critical infrastructure, we initiated this audit to determine whether Bonneville's cyber security program adequately protected its data and information systems.

RESULTS OF AUDIT

Bonneville had taken steps designed to strengthen its cyber security program. Our review, however, identified risk management weaknesses related to the C&A of Bonneville's critical information systems. If not adequately addressed, these weaknesses could adversely impact the security of Bonneville's critical systems and the data they contain. 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 U.S. – 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. Without improvements, Bonneville's systems, including those that support the western energy control area's critical infrastructure, may not be adequately protected from external attacks, insider threats, or inadvertent mistakes.

To its credit, Bonneville had recognized problems with its cyber risk management program and was taking action to address certain weaknesses. For instance, it was working to formally re-approve certain systems for operation through the C&A process. In addition, Bonneville noted that it had begun development of cyber security manuals designed to define security responsibilities for system and information owners and continued to maintain strong controls against network system intrusions.

These actions are positive steps that should help Bonneville strengthen the protective measures applied to its critical information systems. Our report contains several recommendations for additional action that, if fully implemented, should help Bonneville improve its overall cyber security posture.

MANAGEMENT REACTION

Management concurred with the report's recommendations and pledged to correct problems with its cyber risk management program. Bonneville acknowledged risk management problems, however, it noted that C&A, while important, is but one part of its overall cyber security program. Management's comments and our response are more fully discussed in the body of the report. Management's comments are included in their entirety in Appendix 3.

Attachment

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

REPORT ON CYBER SECURITY RISK MANAGEMENT PRACTICES AT THE BONNEVILLE POWER ADMINISTRATION

TABLE OF CONTENTS

Protection of Information Systems

Appendices

Ensuring Security over Information Systems

The certification and accreditation (C&A) process is designed to ensure that information systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The C&A process includes formal steps to recognize and address risks, determine whether system security controls are in place and operating effectively, and ensure that changes to a system are adequately tested and approved. The National Institute of Standards and Technology (NIST) emphasizes the importance of an effective C&A process when developing and implementing information systems. Specifically, NIST notes that "The successful completion of the security certification and accreditation process provides agency officials with the necessary confidence that the information system has adequate security controls, that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and that appropriate plans and funds have been identified to correct any deficiencies in the information system." Reporting instructions published annually by the Office of Management and Budget (OMB) for the Federal Information Security Management Act require that Federal organizations adhere to NIST cyber security related directives/guidance.

Our review of the Bonneville Power Administration (Bonneville or BPA) revealed, however, that it had not fully implemented Federal requirements for certifying and accrediting a number of its systems. Specifically, we noted that responsible officials had not always identified and addressed system risks and system security plans were either not developed or were missing descriptions of key controls needed to protect information. In addition, testing of security controls was sometimes not conducted, insufficient, or was not appropriately documented. Corrective action plans were also not always developed to address identified weaknesses in a timely manner.

Risk Identification and Mitigation

Although specifically required by Federal and Department of Energy (Department) directives, responsible officials had not always ensured that risks to information systems were appropriately identified and mitigated. Specifically, we found that formal risk assessments had not been conducted and/or finalized and that contingency plans had not always been developed to address recovery from a system disruption. In particular, a formal risk assessment had not been completed for any of the four systems we reviewed. Although a draft assessment was prepared for the Control Center System (CCS) more than a year prior to our review, 5 of the 14 identified risks were missing key elements such as the analyses of vulnerabilities and their related impact. In addition, the CCS risk assessment was never finalized.

While a report developed by the certification agent attempted to analyze risks, it excluded information associated with NIST controls relevant to identification and authentication, physical and environmental protection, and systems and communications protection even though these areas had controls described as failing during certification testing. The report also disclosed that without complete risk information, "it is difficult to objectively assess the validity and veracity of existing security controls and control enhancements, and to recommend those which will most effectively mitigate risks to the information system." Due to the lack of adequate risk assessments, Bonneville may not have been able to effectively detect risks associated with the systems we reviewed.

In some circumstances, Bonneville had not developed adequate contingency plans to ensure that information systems and data could be recovered in the event of a significant outage or disaster. For example, plans had been developed for only two of the four systems reviewed. However, one of the plans was never completed and the other did not cover more than 30 sub-systems. Subsequent to our site visits, Bonneville developed plans for 12 major sub-systems included in the CCS; however, plans for 22 other sub-systems remained incomplete. Although Bonneville commented that recovery strategies were in place for the remaining sub-systems, our review of the contingency plan for the CCS revealed that these systems were not specifically covered by the plan. We also noted that Bonneville had not developed a business impact analysis to determine the impact to operations in the event of a disaster and to aid in prioritizing system restoration activities.

Security Planning

We also identified problems with the security planning process at Bonneville. Specifically, Bonneville allowed system accreditations to expire and had not developed security plans for all systems. Even when developed, plans for each of the systems reviewed did not always provide information relevant to system-specific risks or controls to be implemented. For instance:

- While systems should be re-accredited for operation at least once every three years to account for changes in technology and related risks, Bonneville had permitted accreditations to expire for two of four systems reviewed. Bonneville officials noted that the systems with expired accreditations had been incorporated into another larger system and they had initiated action to re-accredit the larger system. However, the decision to incorporate the systems was not made until four months after the accreditations expired. The effort to re-accredit the system remained incomplete at the time we completed our review.

- Security plans had not been developed for various systems at Bonneville. NIST directs that major applications have their own security plan that describes relevant controls, including those that are inherited from a larger security plan. However, even though the CCS contained at least 12 major sub-systems, including those that contributed to the reliability of grid operations, security plans had not been developed to define control requirements unique to those systems. In addition, our review of the larger security plan revealed that it did not adequately describe which controls were to be inherited by the major sub-systems. The importance of developing system-specific plans was emphasized in a May 2007 report prepared by Bonneville system owners and the certification agent that disclosed that 144 of 235 system controls (61 percent) had findings associated with them and included a recommendation that security plans be developed for the 12 major sub-systems.

- Even when security plans were developed, they generally were incomplete and lacked descriptions of how minimum security controls were implemented to meet Federal requirements. Specifically, plans for all four systems reviewed excluded information critical to assessing risks to systems. For example, the security plan for the

CCS did not adequately describe certain controls to be implemented in the areas of access controls and configuration management. Our review of the Business Information Technology (IT) Infrastructure System disclosed that officials had not documented, and were not aware of, the number of sub-systems and applications residing within this plan.

Security Control Testing

Additionally, we identified problems with security control testing for each of the systems reviewed at Bonneville. Specifically, certification testing – a detailed review of an information system's security controls generally performed every three years – was either not performed or not adequately conducted. Required annual self-assessments of security controls were also not always completed. Without adequate control testing, management lacked assurance that security controls were operating as intended.

We found that although Bonneville conducted control testing on its overall general support systems during the initial system certification activities, it did not test the effectiveness of controls on major sub-systems. In cases where certification testing occurred, it was sometimes inadequate or conclusions reached did not reflect the status of the control environment. For instance, we identified 29 controls for the CCS that were rated as passing by the certification agent even though the system security plan and/or self-assessment documentation disclosed that the controls were not in place. Similar disparities were noted on the Business IT Infrastructure System. As a result, Bonneville officials may have been prevented from effectively taking corrective actions to address weaknesses in system controls because they lacked data on specific weaknesses that could have been exposed by testing.

Although NIST notes that an effective information security program includes testing and evaluation of security controls at least annually, Bonneville had not conducted thorough annual self-assessments on any of the systems reviewed in years when certification testing had not occurred. We noted that Bonneville had implemented a continuous monitoring program that always assessed the same subset of controls each year. However, cyber security officials estimated that these assessments only tested about 20-25 of the 235 controls included in NIST Special Publication 800-53. As such, this process did not meet the OMB requirement that "Agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year accreditation cycle."

Corrective Actions

Although OMB requires that plans of action and milestones (POA&M) be developed to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems, Bonneville had not always developed plans to address weaknesses in a number of control areas. Specifically, adequate POA&Ms or corrective action plans to track its efforts for correcting all identified weaknesses had not been developed. In particular, although a POA&M was developed for the CCS, detailed corrective action plans were not established for various weaknesses to show what tasks were to be completed, when they were to be completed, and who was responsible for monitoring the corrective actions. Bonneville also did not develop similar plans for its other systems. Absent adequate corrective action plans, Bonneville may have difficulty managing its progress towards eliminating gaps between required security controls and those that are actually in place.

Security Approach and System Owner Involvement

Many of the weaknesses identified occurred because management had not fully adopted a risk-based approach for identifying and implementing security controls over its information systems in accordance with Federal requirements. In addition, inconsistent involvement from system and information owners contributed to inadequate documentation and testing of cyber security controls.

Risk-Based Approach

Although required by NIST, Bonneville management did not emphasize the importance of utilizing a risk-based, life-cycle approach to manage cyber security. In particular, Bonneville addressed security plans and tested the controls only during the certification process, which generally occurs only every three years. For instance, Bonneville had temporarily assigned an individual to develop the system security plan and assess security controls for the Business

Enterprise System in 2004. However, after completing these activities, he was assigned to work elsewhere and no replacement was ever assigned to continue monitoring security controls.

Additionally, responsible officials had not appropriately prioritized the application of resources towards cyber security activities to ensure an effective cyber security program. For example, key Bonneville executives and managers chose to dedicate resources to identifying and testing certain controls to meet the requirements of OMB Circular A-123 and North American Electric Reliability Corporation critical infrastructure protection standards. However, this effort did not comport with NIST requirements in that it did not ensure that cyber security controls on all systems within the organization were adequately implemented and tested.

Bonneville officials acknowledged that the Administration needed to improve its C&A process but believed that C&A was but one component of its overall cyber security program. Management told us that in spite of the problems we identified with its risk management process, its systems were not in imminent danger of compromise. Bonneville noted that penetration and vulnerability testing performed by the Department's Office of Health, Safety and Security (HSS) in March 2007 had failed to gain control over its critical systems, including those that control power distribution. Although HSS did not gain control of any systems during the March 2007 testing, it did identify a number of high-risk configuration weaknesses and noted that "BPA had not fully considered cyber threats to the *Control Center Network* in their threat assessments and threat statement so that they can conduct valid risk assessments to identify and mitigate cyber security risks." While Bonneville commented that it had developed strong technical controls, a robust C&A process is necessary to ensure that such controls remain effective, adequately address risks, and are changed as needed over the system life cycle.

System and Information Owner Involvement

Although NIST directs that information and system owners actively participate in the security planning process, Bonneville did not adequately involve these key individuals in planning and developing controls. System and information owners, who are not a part of the cyber security function, have the most direct knowledge of the system and the information it contains and also have primary responsibility for determining access and securing these resources. However, these key individuals were not consulted when deciding what security controls should be in place to protect systems or to ensure that the controls were operating as intended. Bonneville did not ensure that system and information owners devoted adequate attention toward securing the systems that protected critical information. Those individuals who had system and information owner responsibilities, such as developing security plans and risk assessments, had not been identified. Rather, Bonneville inappropriately left such tasks to its already small cyber security staff. To its credit, Bonneville had begun to develop cyber security manuals to identify security responsibilities for system and information owners.

Information Security and Assurance

Without improvements, critical information systems maintained by Bonneville to protect national and economic security and contribute to public safety and health could potentially be disrupted. The need for a strong risk-management program becomes apparent when one considers that the number of cyber security incidents reported to the Department's Computer Incident Advisory Capability is at its highest level in three years. A further illustration of the importance of a robust cyber security program is shown in the results of a 2004 report regarding inappropriately protected systems. The report noted that the number of externally generated cyber incidents related to control systems had increased significantly in past years. In addition to these reported external attacks, Bonneville's systems could also be impacted by inadvertent or malicious acts of insiders, or disgruntled former employees. Without complete information, individuals responsible for approving systems for operation may continue to do so without fully understanding the risks associated with not implementing certain security controls.

RECOMMENDATIONS

To address the issues identified in this report, we recommend that the Bonneville Administrator:

1. Establish a risk-based, life-cycle approach for implementing its information security program that allows management and information owners to make informed and cost-effective decisions, to include:

a. Ensuring risks to information resources are assessed periodically, including development of contingency plans;

b. Fully developing security plans and ensuring that systems are timely accredited for operation;

c. Verifying that necessary security controls are sufficiently tested for each system, to include conducting annual control assessments and ensuring that conclusions reached are supported by the test results; and,

d. Maintaining a complete POA&M, to include updated corrective action plans for all identified weaknesses.

2. Re-evaluate how to apply entity resources toward information security program efforts, to include actively engaging system and information owners outside of the cyber security function in risk-based decisions.

MANAGEMENT REACTION

Bonneville expressed concerns with some of the assertions made in the report, but concurred with the recommendations and indicated that it would develop a plan of action to address each of the identified weaknesses. Although Bonneville believed that it had an adequate risk assessment process, management agreed that it did not have sufficient risk-based C&A documentation and disclosed that it would work towards ensuring that systems are both secure and fully documented. Management also commented that it had made a number of improvements that should enhance its cyber security program.

AUDITOR COMMENTS

Management's proposed and stated actions are responsive to our recommendations. We continue to believe that the implementation of strong risk management and C&A processes will enhance Bonneville's ability to protect it systems. As noted by OMB in its Federal Information Security Management Act reporting instructions, the C&A process provides a systematic approach for assessing security controls to determine their overall effectiveness, which is critical to determining the risk to an organization's operations and assets.

Appendix 1

OBJECTIVE

To determine whether the Bonneville Power Administration (Bonneville) cyber security program adequately protected its data and information systems.

SCOPE

The audit was performed between October 2007 and August 2008 at the Bonneville corporate offices.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal regulations, Department of Energy (Department) directives, critical infrastructure protection standards, and guidance pertaining to certification and accreditation of information systems;
- Reviewed prior reports issued by the Office of Inspector General, the Government Accountability Office, and the Department's Office of Health, Safety and Security;
- Reviewed program-level policies relevant to security of information systems;
- Held discussions with program officials from Bonneville; and,
- Selected four systems for review to determine whether relevant cyber security requirements had been implemented.

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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We also assessed performance measures in accordance with the *Government Performance and Results Act of 1993* relevant to security over information systems. We found that Bonneville had not established measures specific to this area. We did not rely on computer-processed data to satisfy our audit objective. Bonneville waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0782, December 2007). The Office of Inspector General (OIG) identified seven significant management challenges facing the Department of Energy (Department), including cyber security. The report noted that although the Department had in place an aggressive effort to address existing weaknesses, we continued to identify deficiencies, including problems relevant to the Department's certification and accreditation (C&A) of unclassified information systems.

- *Audit Report on Continuity of Operations at Bonneville Power Administration* (DOE/IG-0781, November 2007). The OIG found that the Bonneville Power Administration's (Bonneville) continuity of operations capability was not fully compliant with Federal requirements. Specifically, Bonneville (1) needed to improve its alternate operating capabilities for power scheduling and transmission scheduling; (2) did not have specific devolution plans for power scheduling, transmission scheduling, and system operations; and, (3) could not always provide evidence that its Continuity of Operations Planning capabilities were periodically tested or that lessons learned were identified and implemented.

- *Evaluation Report on the Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007). The evaluation identified continued deficiencies in the Department's cyber security program that exposed its critical systems to an increased risk of compromise. In particular, weaknesses existed relevant to system C&A, contingency planning, access controls, configuration management, and change controls. Problems occurred, at least in part, because Department organizations had not always ensured that Federal requirements, Department policies, and cyber security controls were adequately implemented and conformed to Federal requirements, most notably by field organizations and facility contractors.

- *Audit Report on Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Many systems were not properly certified and accredited prior to becoming operational. For example, 9 of 14 sites reviewed had not always properly categorized security levels or risk of damage to major or general support systems and information contained within, or had not adequately tested and evaluated security controls. In many instances, senior agency officials accredited systems although required documentation was inadequate or incomplete, such as incomplete inventories of software and hardware included within defined accreditation boundaries.

- *Audit Report on Management Controls over Selected Departmental Critical Monitoring and Control Systems* (OAS-M-05-06, June 2005). The OIG found that the Department could not ensure that it could continue operations or quickly restore selected critical monitoring and control systems in the event of an emergency. Specifically, management had not fully assessed risks or taken adequate steps to mitigate the foreseeable risks confronting the six critical monitoring and control systems reviewed. This issue occurred because site management had not sufficiently considered and periodically evaluated the risk that critical monitoring and control systems would become inoperable and unable to be restored in a timely manner.

- *Audit Report on Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003). Western Area Power Administration (Western) and Southwestern Power Administration had not adequately assessed the vulnerabilities and risks for their critical assets. Vulnerability and risk assessments at Western were inadequate because management was primarily concerned about recovering from any disruption in operations, regardless of its source.

Appendix 3

Department of Energy

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

EXECUTIVE OFFICE

[illegible] 2008

In reply refer to: J-3

MEMORANDUM FOR RICKY R. HASS, IG-34 (A08TG039)
ASSISTANT INSPECTOR GENERAL FOR ENVIRONMENT, SCIENCE, AND CORPORATE AUDITS

FROM: STEPHEN J. WRIGHT
ADMINISTRATOR AND CHIEF EXECUTIVE OFFICER

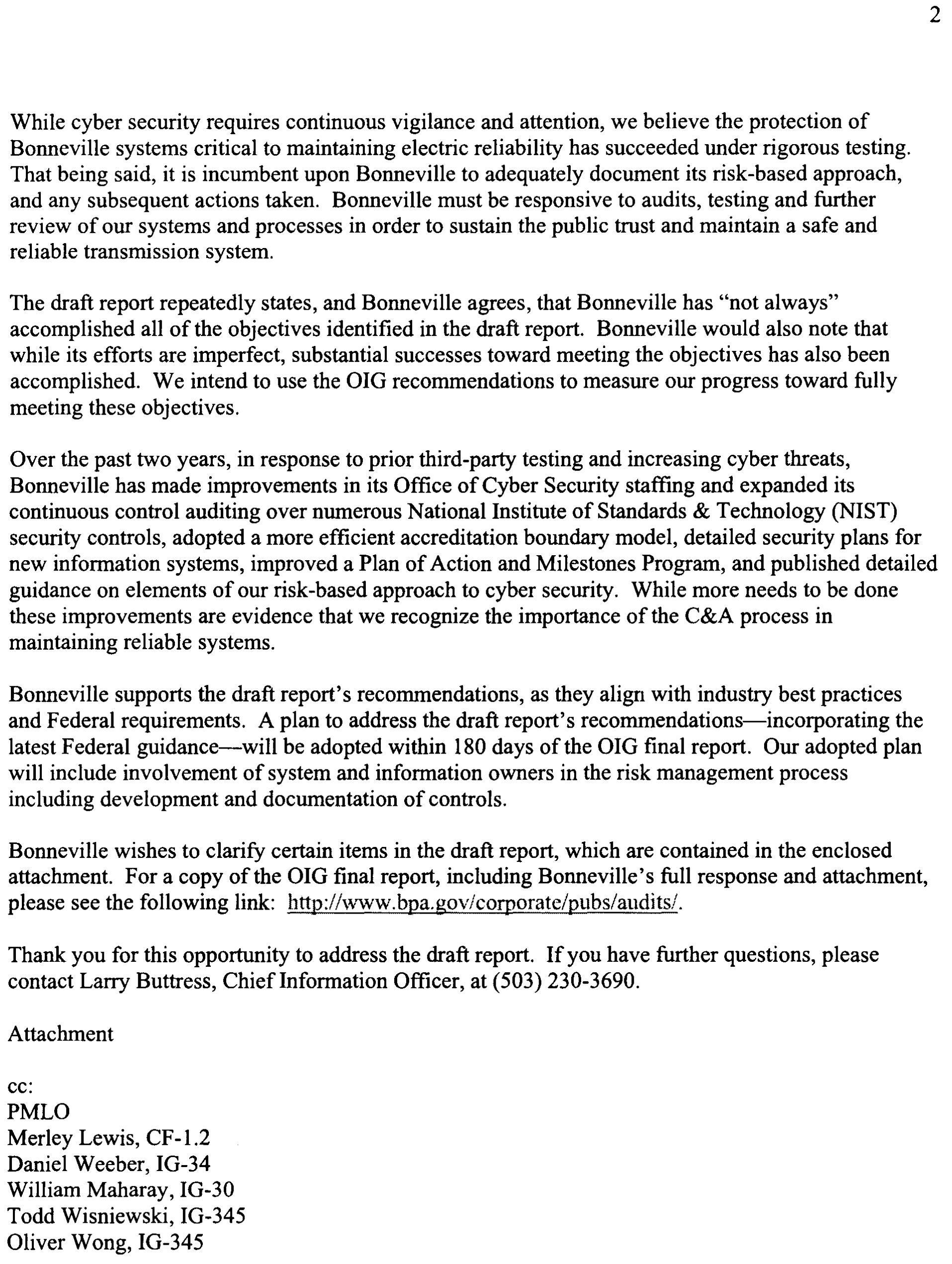
SUBJECT: RESPONSE TO DRAFT AUDIT REPORT ON "CYBER SECURITY RISK MANAGEMENT PRACTICES AT THE BONNEVILLE POWER ADMINISTRATION"

The Bonneville Power Administration (Bonneville) appreciates the opportunity to comment on the draft report of the subject audit. While we have concerns with some of the assertions in the body of the report, we generally agree with the Office of Inspector General's (OIG) recommendations. The recommendations will assist us in improving the Certification & Accreditation (C&A) elements of our cyber security program.

Bonneville places a very high priority on assuring the reliability and security of its electric power grid. This led us to establish a robust and effective agency cyber security program. That program continues to be improved as new needs are assessed. We recognize the importance of the C&A process in maintaining reliable systems, and as the draft report states, Bonneville has made significant improvements in our cyber security program. We also recognize that our C&A program must continue to improve.

In the draft report, the audit team concluded that Bonneville did not have sufficient risk-based C&A documentation. Bonneville agrees. There is, however, a distinction between C&A documentation requirements, which were tested by the audit team, and the adequacy of security controls protecting our information systems. C&A documentation by itself does not ensure that a system is secured. An unsecured system may have excellent documentation while a secure system may have little documentation. Bonneville supports the goal of secure systems that are fully documented and continuously assessed. Bonneville will use this report in order to work towards those goals.

Bonneville's security controls have successfully withstood intensive external penetration testing during past cyber security evaluations by the DOE Office of Cyber Security Oversight (HS-62). In each case, the oversight team was unable to penetrate protective measures or gain unauthorized access to our mission-critical systems and networks, including those which control Bonneville's electric power grid. This effort also identified potential cyber control weaknesses, which Bonneville has addressed or reported for corrective action.



While cyber security requires continuous vigilance and attention, we believe the protection of Bonneville systems critical to maintaining electric reliability has succeeded under rigorous testing. That being said, it is incumbent upon Bonneville to adequately document its risk-based approach, and any subsequent actions taken. Bonneville must be responsive to audits, testing and further review of our systems and processes in order to sustain the public trust and maintain a safe and reliable transmission system.

The draft report repeatedly states, and Bonneville agrees, that Bonneville has "not always" accomplished all of the objectives identified in the draft report. Bonneville would also note that while its efforts are imperfect, substantial successes toward meeting the objectives has also been accomplished. We intend to use the OIG recommendations to measure our progress toward fully meeting these objectives.

Over the past two years, in response to prior third-party testing and increasing cyber threats, Bonneville has made improvements in its Office of Cyber Security staffing and expanded its continuous control auditing over numerous National Institute of Standards & Technology (NIST) security controls, adopted a more efficient accreditation boundary model, detailed security plans for new information systems, improved a Plan of Action and Milestones Program, and published detailed guidance on elements of our risk-based approach to cyber security. While more needs to be done these improvements are evidence that we recognize the importance of the C&A process in maintaining reliable systems.

Bonneville supports the draft report's recommendations, as they align with industry best practices and Federal requirements. A plan to address the draft report's recommendations—incorporating the latest Federal guidance—will be adopted within 180 days of the OIG final report. Our adopted plan will include involvement of system and information owners in the risk management process including development and documentation of controls.

Bonneville wishes to clarify certain items in the draft report, which are contained in the enclosed attachment. For a copy of the OIG final report, including Bonneville's full response and attachment, please see the following link: http://www.bpa.gov/corporate/pubs/audits/.

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.

Attachment

cc:
PMLO
Merley Lewis, CF-1.2
Daniel Weeber, IG-34
William Maharay, IG-30
Todd Wisniewski, IG-345
Oliver Wong, IG-345

IG Report No. DOE/IG-0807

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 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 Judy Garland-Smith (202) 586-7828.