



## Department of Energy

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

EXECUTIVE OFFICE

NOV 20 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

## ATTACHMENT

The Bonneville Power Administration (Bonneville) responded to the Department of Energy (DOE) Office of the Inspector General (OIG) draft audit report titled, “Cyber Security Risk Management Practices at the Power Marketing Administrations,” in the two pages to which we were limited. A more detailed discussion and clarification of issues raised by the report follows below.

### **1. The draft audit report will guide Bonneville’s interpretation of NIST guidelines to meet Federal requirements.**

The draft audit report states [Ensuring Security over Information Systems section, Paragraph 2]:

*“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.”*

Implementation, of NIST Special Publications (SP) requires agencies to use judgment therefore some interpretation is necessary. NIST states<sup>1</sup>, “When assessing agency compliance with NIST guidance, auditors, evaluators, and/or assessors should consider the intent of the security concepts and principles articulated within the particular guidance document and how the agency applied the guidance in the context of its specific mission responsibilities, operational environments, and unique organizational conditions.” Bonneville included these elements in our interpretation and implementation of applicable Federal requirements. The entire audit process as well as the draft audit report have been and will continue to be helpful as additional element to guide Bonneville’s improvement of its Risk Management program for cyber security.

### **2. Bonneville has tested security controls in accordance with National Institute of Standards & Technology (NIST) guidance, both as a component of the C&A process, and on a continuous basis as a component of a methodical continuous monitoring program.**

The draft audit report states [Ensuring Security over Information Systems section, Paragraph 2]:

*“...testing of security controls was sometimes not conducted, insufficient, or was not appropriately documented.”*

Bonneville regularly tests NIST security controls for the identified risks that affect its systems based on upon the guidance from NIST quoted in item # 1 of this attachment. .

### **3. The draft audit report makes an assertion that Bonneville did not adequately assess the risk for its information systems.**

The draft audit report states [Risk Identification and Mitigation section, Paragraph 1]:

---

<sup>1</sup> NIST SP 800-53 Rev2, Recommended Security Controls for Federal Information Systems

*“ . . . formal risk assessments had not been conducted and/or finalized and that contingency plans had not always been developed to address recovery from system disruption. In particular a formal risk assessment had not been completed for any of the four systems we reviewed.”*

The draft audit report does not define or qualify what constitutes an adequate risk assessment and does not state the standard against which Bonneville’s risk assessments were measured. Bonneville currently has two information systems reportable under the Federal Information Security Management Act (FISMA). The confusion in the draft audit report stems from the fact that the audit team reviewed C&A documentation from years past. A formal risk assessment is conducted for all FISMA reportable systems in accordance with NIST Special Publication (SP) 800-30.

One criticism the audit team made regarded Bonneville’s Control Center System (CCS) draft Risk Assessment Report. The report was mislabeled “draft” and yet it contains extensive, valuable and relevant vulnerability information, and guides current Bonneville corrective actions. The Risk Assessment Report describes nine Risk Areas, each with a “Vulnerability Analysis” and an impact rating. It also includes an impact analysis. Reports such as this are not formally published but considered working papers.

The draft audit report’s statement that the risks are “missing key elements” is not relevant to the residual risk of the CCS. The important risk elements are specifically identified in Bonneville’s document titled “Certification Report,” which highlights residual risks associated with continued operation of the CCS and identified corrective actions to be undertaken.

Bonneville has performed extensive risk assessments that meet the objectives of identifying residual risks to the responsible official with approval authority. The entire body of C&A documentation speaks to and provides evidence of this risk assessment activity. For instance, a second method of risk assessment was also formally applied to the CCS which included a documented review of 235 controls and control enhancements from NIST SP 800-53. The review took place over several months, wherein sub-system managers and qualified information security professionals worked together to analyze every control to assess how any potential threat might compromise the systems confidentiality, availability or integrity. The results were documented in the self-assessment checklist and used by the certification agent in assessing in-place controls.

The C&A process and cyber security program at Bonneville is founded upon risk assessment and risk management. The Bonneville Office of Cyber Security is staffed with information security officers, information security specialists, and certified computer forensic examiners who are all required to maintain industry standard certifications. This staff assesses risks to Bonneville information systems on a continuous basis.

#### **4. The draft audit report misunderstands statements about a lack of risk assessment information from Bonneville’s Certification Agent.**

[Risk Identification and Mitigation section, Paragraph 1 last sentence.]:

*“In addition, a report developed by the certification agent for this system noted that ‘A fundamental challenge in assessing the security controls for the CCS was a near total lack of internal and external risk assessment information.’”*

The statement is a reference to a lack of valid external threat information, which would ordinarily be obtained from intelligence agencies, law enforcement, or Department of Energy (DOE) headquarters, and would contain timely information on threats that directly apply to the Power Marketing Administrations generally and Bonneville in particular. Bonneville has yet to find a source for such information.

**5. The draft audit report does not reflect actions taken by Bonneville in accordance with NIST guidance to incorporate major applications and sub-systems into general support systems, and inappropriately counts systems no longer in operation.**

The draft report states [Security Planning section, 1<sup>st</sup> bulleted paragraph]:

*“Bonneville had permitted accreditation to expire for two of four system reviewed. Bonneville officials noted that the systems with expired accreditations had been incorporated into another larger system, and they had initiated action to reaccredit the larger system.”*

Of the two systems that the draft audit report noted had expired accreditations, one is no longer in operation and the functionality of the other has been incorporated into a general support system in accordance with NIST guidance. Bonneville performs re-accreditations either within the prescribed three-year cycle or more frequently, as warranted by circumstances. Bonneville currently has two FISMA reportable general support systems, each with a valid Authority to Operate.

**6. Bonneville believes that security control requirements for its information systems are defined in accordance with NIST requirements and guidance.**

The draft report states [Security Planning section, 2nd bulleted paragraph]:

*“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, as required by the National Institute of Standards and Technology (NIST).”*

Bonneville has developed security plans for information systems that contribute to the reliability of the electric power grid. The twelve sub-systems referenced in the draft report inherit their security controls from the CCS general support system, as documented in the CCS System Security Plan.

**7. The draft audit report incorrectly states that critical information needed to assess cyber security risks was excluded.**

The draft report states [Security Planning section, 3<sup>rd</sup> bulleted paragraph]:

*“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 at each of the 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, configuration management and media protection.”*

The requirements the auditors found lacking were paperwork and documentation. NIST Special Publications are required by OMB and therefore are a Federal requirement. However, these publications are written as guidelines, which Bonneville believes cannot be evaluated or measured without considerable interpretation. The OIG presents one such interpretation. Not all security controls must be addressed or present in all systems, which NIST refers to as *“control tailoring and scoping.”*

In specific examples that the draft audit report describes (Media Protection, Access Control and Configuration Management) it is unclear why the draft audit report is critical. All three of these control families were identified in the Certification Agent Report, which was shared with the audit team, and were reported by Bonneville to the DOE as corrective action items in the Plan of Action and Milestones report. In other words, Bonneville had formally identified and reported weaknesses as required by DOE in accordance with NIST guidance.

In the area of Media Protection in the CCS at the time of the audit, Bonneville had and continues to have a media protection process that meets or exceeds DOE requirements. As a component of this process, Bonneville routinely samples and forensically tests hard disk drives which have been wiped or purged. No hard drives leave the facility unless wiped or purged in accordance with DOE requirements. Access Control and Configuration Management were similarly well implemented at the time of the audit, but areas for improvement were noted and reported.