Department of Energy

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

EXECUTIVE OFFICE

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-

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.

Sincerely,

Stephen J. Wright
Administrator and Chief Executive Officer

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