Bonneville's Responses to the IG's Draft Audit Report

This appendix supports Bonneville's response to the Inspector General's Draft Audit report: *Management of Bonneville Power Administration's Information Technology Program*. It is intended to correct several erroneous assertions made in the report and provide interested parties with additional information regarding the effectiveness and efficiency of BPA's IT program. Our program follows a continuous improvement process and uses the agency's balanced scorecard to measure progress. We believe the material provided below will provide a broader sense of the quality of our program, as we respond to specific statements made in the draft OIG's report.

The items below are listed in the order in which they were mentioned in the OIG's draft report.

Statement: Testing identified 11 servers that were configured with weak passwords

BPA Position: Agree – A standard password complexity policy will be developed.

Pertinent Facts: The Administrative account in question used a password that met industry established levels of complexity on the specified servers. This is the default password the server team uses to build the system from scripts. The issue here is not in the strength of the password but rather that the password was not changed prior to moving into production. Bonneville agrees a policy must be put into place to address a standard password complexity and related processes for bringing servers into the production environment.

Statement: 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.

BPA Position: Agree – But, further clarification needed (see below);

Pertinent Facts: The 400 number is duplicative, and actually indicates 103 unique vulnerabilities, with the largest majority being outdated versions of the HP System Management application. The remaining 11 vulnerabilities have been remediated.

Statement: … 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 Bonneville told us that it was aware of the outdated software issue and that efforts were underway prior to the audit to migrate the servers to a current software version.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.

BPA Position: This effort, where applicable, was already underway prior to audit.

Pertinent Facts: A number of the applications running on these systems require an old Windows 2000 platform and have no capability to be migrated to a current operating system. This is simply a fact of life for some of the older applications in our production environment.

Statement: … we found that Bonneville had developed and implemented standard configurations for only two of its four server operating systems.
BPA Position: This effort was already underway prior to audit.

Pertinent Facts: Bonneville agrees with this finding, however, the two operating systems (WIN2003 and WIN2008) utilizing standard configurations constitute over 96% of all our server operating systems. Additionally, since the IG audit we have developed and implemented a standard for the Linux OS. This leaves only the Solaris OS as the one outstanding OS without an established standard, a shortcoming that will be resolved by the end of Q3 FY12.

Statement: …12 instances where regular users had been assigned administrative privileges to servers based on group membership.
BPA Position: Agree – Privileges will be removed;

Pertinent Facts: This refers to a list of users whose accounts had administrative privileges through group membership. Whether or not the users needed these privileges is opinion, but that opinion is based on the table of information provided to the OIG by BPA, based on those descriptions, we conclude that only 3 of the 12 should have administrative privileges.

Statement: … only two of six systems had contingency plans that were documented and tested for effectiveness.
BPA Position: This effort was already underway prior to audit.

Pertinent Facts: Asset Management and Engineering (AME) is a system of systems as is the Information Technology Infrastructure (ITI) system. These two collections of system meet the definition for general support system described in government regulations and are groupings used for governance and compliance under the Federal Information Security Act (FISMA) they are not systems that would have a monolithic plan for contingencies. Some of the subsystems in AME, do not require detailed contingency plans as they are already distributed systems with automatic failover or simply are not of high enough categorization to be of concern. The ITI is the infrastructure itself, which includes an alternate data center.

AME and ITI then are large groupings of individual applications and infrastructure, ProjectWise is a subsystem within AME and GRC is a Software as a Service system. Although formal contingency plans do not currently exist BPA IT has processes in place that have been tested for the business and administrative infrastructure (the ITI) on which the majority of BPA IT systems rely including AME; tape back-ups and off-site storage provide a common strategy for contingencies which nearly all of these system inherit. BPA IT is committed to getting formal contingency plans in place for the infrastructure and business systems as resources allow.

Statement: … 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. Specifically, 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 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.

BPA Position: Agree – but, further clarification needed (see below);

Pertinent Facts: Cost figures contained in the report are misleading. The $4.5m figure was an initial projection at project inception. The Planning Stage forecast was $7.4M. After final vendor selection and negotiations, and completion of planning activities, the approved cost was $8.3M.

The project was successfully delivered, consistent with the CAB-approved (Capital Allocation Board) business case.

The delta in project costs ($8.3m at the end of planning and $11.5m provided as final costs) were approved by executive sponsors and formal project oversight committees – once approved the project was managed and delivered according to the approved values.

Statement: …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.

BPA Position: Agree - But, further clarification needed (see below);

Pertinent Facts: The fact that 'only one office had access to and was utilizing the system.' was based on Bonneville's decision to focus on the compliance aspects of the software package in support of the NERC-CIP certification process over the Internal Audit and A123 aspects as it was deemed a higher business priority.

Statement: … 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 five 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.

BPA Position: Disagree

Pertinent Facts:

Project delay - Resources were reallocated causing a delay in the project based upon management's decisions to allow the DLS project to idle while more critical projects were completed, including the WECC No Sanctions, WECC EIDE Interface, and NERC CIP implementation. In addition, the original project scope was expanded to include 2 system replacements (DLS and COMPASS) rather than just one.

Scope changes-

Changes to project scope, schedule and budget are made only by project sponsors, and are based on risk and cost benefit decisions. The changes to scope in this project were approved by the project sponsors (managers and executives within the System Operations organization) representing the end users and automation support staff.

Statement: … Bonneville had purchased several types of software over the past three years 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.

BPA Position: Agree - But, further clarification needed (see below);

Pertinent Facts: Bonneville's Approved Software List contains titles that are approved for installation into the Agency's production environment. It is not a list of software approved for purchase. This is an important distinction in understanding the OIG's report.

Some software titles identified in the report, as not being on the Approved Software List, are just variations of titles (e.g. Hummingbird Exceed vs. Exceed).

It's important to note that vendors normally sell only the current version of a given software license. This means, to ensure license compliance, we must buy the currently available version, yet install the previous (approved) compatible version for the client.

Statement: …about 50 percent of software purchased by TO was not on approved software list, compared with only 7 percent for the rest of BPA

BPA Position: Agree – Effort will be undertaken;

Pertinent Facts: We generally agree that the Approved SW List maintained by the CIO's office, does not include software unique to Grid Operations IT. Bonneville will work to incorporate Grid Ops software titles into the Approved SW List, so that one composite standards list governs production software across all Bonneville.

Transmission Operations (TO) purchases software via the standard supply chain purchasing processes through the use of a TRR (Technology Resource Request) form. Some software purchases are done via the contracting office as a standard contract agreement. The TRR process has stopped or changed some software requests that were not on the approved software list. There are a few times when TO needs a software product not on the approved list, but is allowed to purchase since the product is only to be used in the control center environment. TO does keep its own list of software it uses in the control center environment.

Statement: 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.

BPA Position: This effort was already underway prior to audit.

Pertinent Facts: We generally agree that Bonneville needs a more effective patch management program. To that end, we have a Patch Management Improvement Project underway.

As part of our Agency IT Patch Management Capital project for FY2012, the project team along with the Infrastructure Admin Services team, will educate each of the identified ISOs of their responsibility for patch management along with the capabilities of the new patch management system being implemented. This will also afford an opportunity for IT to address ISO responsibilities for additional security controls.

Statement: **…**multiple system owners commented that the responsibility for contingency planning efforts rested with Bonneville's Office of Business Continuity.

BPA Position: Agree - Effort underway;

Pertinent Facts: When interviewed, some BPA employees incorrectly responded with these statements. They could have been referring to the responsibility of the BC group to drive the overall Business Continuity program, but still the response is incorrect. Bonneville will redouble efforts to ensure Information System Owners fully understand their responsibilities, including Business Continuity planning.

Statement: 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.

BPA Position: Agree – but further clarification needed (see below);

Pertinent Facts: The primary purpose of the Planning Phase in SDLC 1.4 was to do sufficient planning and analysis to develop the business case and support a build versus buy decision. This is important from a capitalization perspective in that once this decision is made, the asset being built is identified and project work from that point forward can be capitalized. Capitalization started in the Execution Phase of a project.

"Section 5.2 Tasks and Activities" in the SDLC 1.4 clearly indicates that the first activities in the Execution Phase of a project are refinement of requirements, design, cost estimates, ROI, and all the associated plans. It goes on to describe that these are precursors to developing, testing and implementing the system. Cost, schedule and scope are not defined during project implementation, but before any development begins.

SLC 2.0, now in effect, further separates the requirements, design and planning activities from implementation activities. The Execution Phase in SLC 2.0 is separated into two phases; System Planning and Execution with a hard "Stage Gate" and assessment process between the two. In System Planning, detailed requirements, designs and implementation plans are developed and in Execution, construction, testing and deployment occurs.

Bonneville believes the issue is not as much about what stage in the project lifecycle detailed requirements, designs and plans occur but rather the rigor with which they are performed and the processes that are in place to ensure consistent application. Evidence of this was provided to the OIG auditors but omitted in the report.

Statement: 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.

BPA Position: Disagree

Pertinent Facts: Section 5.2.6 of the Project Manager's Handbook v7.0 states,
"The PM should make every effort to avoid having to process an IT Project Change Order during the Execution Stage".

And further; "In the event an unanticipated event puts the IT project's committed scope, schedule or budget at risk, the PM must immediately notify the JP-PMO Manager and discuss the options that may be pursued to avoid processing an IT Project Change Order. In the event that JP-PMO Manager believes an IT Project Change Order is necessary, the PM will then be authorized to begin the change order process."

Statement: Specifically, project managers and their teams did not always adhere to SDLC planning requirements and made significant changes to project scope during project execution.

BPA Position: Disagree

Pertinent Facts: Changes to project scope, schedule and costs during the project lifecycle are a fact of life, and such changes as long as they follow proper approvals, do not violate SDLC planning requirements, and are consistent with standard industry practices (i.e. PMI's Project Management Body of Knowledge (PMBOK)).

We also believe the OIG report confuses the SDLC “Execution” phase with “Implementation”.

Statement: …"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."

BPA Position: Agree - Further clarification needed (see below);

Pertinent Facts: The areas of scope removed from the TAS project are still being pursued by the business and the decision of whether or not the Cascade Software Package will be used in these areas has not yet been made. This report finding is incomplete and draws a misleading conclusion.

Statement: … the SDLC did not fully detail the timing of required coordination with cyber security during the project management process.

BPA Position: Disagree

Pertinent Facts: This issue was not a factor on the TAS Project; the handheld units were tested by Cyber Security prior to purchasing them.

Guidance in this area is included in the SDLC. Section 5.4.5, "System Security Plan", of SDLC 1.4 states the following, "Based on BPA F1324.02e. Must be submitted to Cyber Security and signed off by the Authorizing Official prior to start of the Implementation Task (580). After Cyber Security performs Security Testing and Evaluation (ST&E), the SSP is sent as part of a Security Authorization Package to the Authorizing Official who will either issue an Authority to Operate (ATO) or deny the authorization based on the risk involved in operating the system.

BPA hired and assigned Security Engineers to each IT PMO project to ensure appropriate security controls were being implemented, NIST processes were being followed, and that coordination with Cyber Security was occurring.

During FY09 and FY10, Cyber Security coordinated training for IT Operations and PMO management and project teams on NIST SP800-37, Rev 1 for inclusion on IT Projects.

SLC 2.0 became effective in September, 2011 and offers additional cyber security guidance and procedural instructions per NIST SP 800-37, Rev 1.

Statement: 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 that he was working on three projects and did not have sufficient time to spend on managing the project effectively.

BPA Position: Disagree

Pertinent Facts: We dispute this notion that we have inadequate resources to manage Bonneville's IT program. We also believe our project delivery success rate of over 80% is a clear indication that our projects, while lean, are adequately resourced for success.

Statement: In addition, the OCIO did not have purview over IT operations and procurements that were part of Transmission Operations.

BPA Position: Agree - Effort underway;

Pertinent Facts: We generally concur with this assessment. An initiative is underway to extend the OCIO's governance to include Transmission Services IT functions.

END