



Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, N.W., Washington, D.C. 20005-4026

November 18, 2009

Honorable Peter Orszag
Director, Office of Management and Budget
Eisenhower Executive Office Building
725 17th Street, N.W., Room 252
Washington, DC 20503

Dear Mr. Orszag:

The Pension Benefit Guaranty Corporation (PBGC) Office of Inspector General (OIG) contracted with Clifton Gunderson LLP, an independent public accounting firm, to perform, under OIG oversight, the independent evaluation and review of PBGC's information and technology security required by the Federal Information Security Management Act (FISMA), Federal Managers' Financial Integrity Act (FMFIA) and the Office of Management and Budget (OMB). The review assessed the effectiveness of PBGC's information security program and practices and determined compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines. Clifton Gunderson used the Government Accountability Office's (GAO) Federal Information Systems Controls Audit Manual (FISCAM) as well as guidance issued by the National Institute of Standards and Technology to assess the impact PBGC's significant IT systems and operations. Specifically, the areas of review included:

- Entity-wide security program planning and management;
- Access control;
- Configuration management;
- Segregation of duties; and
- Contingency planning.

OMB's new reporting guidelines, as prescribed by Memorandum M-09-29 have directly impacted our responses to a significant number of the FY 09 questions. In past years we did not opine on "adequacy and effectiveness," rather we reached consensus with PBGC at a much higher level. For example; last year we limited our review to determining whether certification and accreditation (C&A) documentation for a system existed. This year we contracted for a detailed assessment of the adequacy and effectiveness of PBGC's information and technology security. A number of significant deficiencies were identified which are reflected in our responses.

PBGC's systemic security control weaknesses and the lack of an integrated financial management system posed increasing and substantial risk to PBGC's ability to carry out its mission during FY 2009. Communication to PBGC's key decision makers did not convey the

urgent need for decisive strategic decisions to correct fundamental weaknesses in PBGC's IT controls and security. Strategic IT decisions did not address these deficiencies and significant weaknesses.

Current year audit work found deficiencies in the areas of security management, access controls, configuration management, and segregation of duties. Control deficiencies were also found in policy administration, and the certification and accreditation of major applications and general support systems. An effective entity-wide security management program requires a coherent strategy for the architecture of the IT infrastructure and the deployment of systems. The implementation of a coherent strategy provides the basis and foundation for the consistent application of policy, controls and best practices. PBGC first needs to develop and implement a framework to improve their security posture. This framework will require time for effective control processes to mature. Based on the current assessment, Clifton Gunderson reported:

- Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for Security Awareness training. PBGC currently has a cumbersome and error prone manual process to account for personnel who have completed security awareness training.
- PBGC's configuration management controls are labor intensive and ineffective. Weaknesses in the design of PBGC's infrastructure and deployment strategy for systems and applications created an environment where strong technical controls and best practices cannot be effectively implemented.
- Controls are not consistently implemented to appropriately segregate duties and grant rights and privileges commensurate with job functions and responsibilities. PBGC does not have a coherent strategy for enforcing segregation of duties through strong technical controls in its applications and general support systems. Developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of applications, the circumvention of critical controls, and unnecessary access to sensitive data.
- PBGC's process for the completion of C&A packages in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* is ineffective. Fundamental weaknesses in PBGC's infrastructure architecture and design do not support the certification and accreditation of its information systems. Furthermore, PBGC's information systems employ obsolete and antiquated technologies that pose additional risk to the availability of financially significant systems. The review determined that only 1 of the 13 C&A packages asserted that were completed in FY 2009 met NIST requirements. Significant deficiencies were noted in access controls and configuration management for the remaining C&A packages.

The OIG and CIO's office worked diligently to reconcile our FY 09 FISMA responses. While we were in agreement on most questions posed by OMB, we did not agree on the number of systems for which contingency plans have been tested in accordance with policy. Specifically, the CIO's office reported testing six systems and OIG reported four. We believe this discrepancy stems from two agency systems that do not have adequate storage capacity or server configurations at the COOP site. Therefore, in our view these systems do not meet the adequacy and effectiveness threshold as prescribed by OMB Memorandum M-09-29, FY 2009 Reporting

Instructions for the Federal Information Security Management Act and Agency Privacy Management.

To its credit, PBGC has taken steps in developing an overall strategy to improve its IT architecture and infrastructure. Major steps include:

- Completing an assessment of its Oracle database environment, initiating an IT Infrastructure modernization program and implementing strategic decisions on IT sourcing.
- PBGC completed the identification of all systems that provide data required to prepare the financial statements.
- PBGC has substantially completed the logical database model including standard data definitions and formats to be used throughout the Corporation.
- PBGC has completed the development of segment architectures for the Consolidated Financial Systems (CFS) and Premium Accounting. Segment Architectures will assist PBGC in identifying and planning financial technology recommendations for implementation and alternative analysis for business cases.

PBGC has made a commitment to have executives at the highest level focus on IT, but much work remains. To further assist PBGC with its security program development and implementation, the OIG will continue to perform independent evaluations on an annual basis in addition to scheduled audits. Our work will include, but not be limited to, the following targeted areas:

- Review of contractor provided services, as well as services from agencies;
- Annual financial statement audit, to include an evaluation of PBGC general and system controls;
- Application reviews, in addition to those included in the annual financial statement audit; and
- Reviews of agency incident handling.

As always, the OIG will continue to work with and support PBGC through our reviews and analysis related to the agency's mission and programs, including information assurance and security.

Sincerely,



Joseph A. Marchowsky
Assistant Inspector General for Audit