



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

November 12, 2010

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

Dear Mr. Zients:

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

PBGC's systemic security control weaknesses and the lack of an integrated financial management system continued to pose increasing and substantial risk to the Corporation's ability to carry out its mission. PBGC's key decision makers are acutely aware of the challenges facing the Corporation in addressing fundamental weaknesses in its IT infrastructure and environment. In past years, PBGC's key decision makers did not communicate the urgent need for decisive strategic decisions to correct these fundamental weaknesses, and the weaknesses were not addressed in the status of corrective actions being reported. Hence, current management has taken a multiyear approach to correct these deficiencies. PBGC management realizes these weaknesses will continue to pose a threat for several years while corrections are implemented.

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. As the Corporation is in the early stages of implementing its corrective action plan (CAP), Clifton Gunderson reported continued deficiencies in the areas of security management, access controls, configuration management, and segregation of duties. Based on the current assessment, Clifton Gunderson also reported:

- PBGC's benefits payment contractor implemented a security operations center outside the United States which will have some responsibility for security events of a particular PBGC application. The service provider did not give the PBGC adequate notice to assess the risk to its systems. As a result, PBGC had not assessed the security impact of the changed environment.
- PBGC relied on hardware and software that was no longer supported by the associated vendors.
- PBGC abandoned its certification and accreditation(C&A) process because fundamental weaknesses in PBGC's infrastructure architecture and design do not support the certification and accreditation of its systems. The Corporation is currently working with the Bureau of Public Debt to revise and strengthen its C&A process in order to ensure security weaknesses are addressed at the root cause level.

To its credit, the Corporation has taken steps to develop and begin implementation of a multi-year CAP to address security issues. The CAP, a 3 to 5 year plan, is part of PBGC's overall strategy to improve its IT architecture and infrastructure. Effective implementation of the CAP will require PBGC's continued efforts to ensure appropriate metrics are in place and milestones are met timely. The CAP includes:

- Implementation of a more effective C&A process,
- Strategies to address fundamental security weaknesses, and
- Initiation of an IT infrastructure modernization program.

PBGC has also procured and installed new hardware into its infrastructure, as it works toward modernization. To further assist PBGC with its security program development and implementation, the OIG will continue to perform independent audits and evaluations.

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

Sincerely,



Joseph A. Marchowsky
Assistant Inspector General for Audit