



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

November 14, 2012

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 CliftonLarsonAllen LLP, an independent public accounting firm, to perform the independent evaluation and review of PBGC's information and technology (IT) security required by the Federal Information Security Management Act (FISMA), Federal Managers' Financial Integrity Act (FMFIA) 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. CliftonLarsonAllen 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.

IT continues to be a challenge for management. The safeguarding of PBGC's systems and data is essential to protect PBGC's operations and mission. The OIG has consistently identified serious internal control vulnerabilities and systemic security control weaknesses in the IT environment over the last several years. PBGC's delayed progress in mitigating these deficiencies at the root-cause level continued to pose increasing and substantial risks to PBGC's ability to carry out its mission during FY 2012. Due to the persistent nature and extended time required to mitigate such vulnerabilities, additional risks threaten PBGC's ability to safeguard its systems. These risks include technological obsolescence, inability to execute corrective actions, breakdown in communications, and poor monitoring.

PBGC has made progress in addressing the design of its infrastructure, account management, enterprise security management, and configuration management, but the control processes have not reached a level of maturity to prove their effectiveness. The Corporation has also developed and is implementing additional policies and procedures. PBGC is in the process of establishing an enterprise-wide continuous monitoring program and deploying additional network management tools. However, much remains to be done, and the pace of progress remains slow.

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