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

November 14, 2014

The Honorable Shaun Donovan
Director
Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Donovan:

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; and
- Incident Response

PBGC has made progress in some areas of IT; yet, as the agency progresses other controls are not being adequately updated to prepare PBGC for future threats. PBGC continues to have significant weaknesses in incident response, continuous monitoring, and common control identification and dissemination. OIG was highly concerned with PBGC's incident response program in FY 2014, specifically an agency-wide phishing incident that was not adequately assessed. We procured Mandiant (a world renowned incident response firm) to conduct a compromise assessment of the PBGC network. No evidence of attacker activity was identified at the time of the assessment (see report summary at http://oig.pbgc.gov/pdfs/Eval-2014-12IT-14-104.pdf). However, Mandiant's findings supported our recommendations and conclusions that PBGC must timely address weaknesses within the incident response program.

PBGC recently hired a new Chief Information Security Officer (CISO), who informed us that a corrective action plan is being developed to address findings and recommendations within incident response. Moreover, the FY2014-2018 *Information Technology Strategic Plan*, finalized in December 2013, prioritized the confidentiality, availability, and integrity of systems and data as the number one goal. Areas of notable improvement in FY 2014 include: Security Authorization and Assessment (SA&A), defining baseline configurations, and implementation of policies and procedures to ensure user access is appropriate.

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,

Rashmi Bartlett
Assistant Inspector General for Audit