Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation Report

Fiscal Year 2013 Federal Information Security Management Act Final Report

March 21, 2014

EVAL-2014-9/FA-13-93-7

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

March 20, 2014

To: Josh Gotbaum
Director

From: Rashmi Bartlett
Assistant Inspector General for Audit

Subject: Fiscal Year 2013 Federal Information Security Management Act Independent Evaluation Report (Eval 2014-09/FA-13-93-7)

I am pleased to transmit the final year (FY) 2013 Federal Information Security Management Act (FISMA) report, detailing the results of our review of the Pension Benefit Guaranty Corporation (PBGC) information security program. As prescribed by FISMA, the PBGC Inspector General conducts annual evaluations of the PBGC security programs and practices, and reports to the Office of Management and Budget (OMB) the results of the evaluation. This evaluation report provides additional information on the results of our review of the PBGC information security program.

PBGC agreed with all recommendations in this report. Though PBGC has made some progress in addressing IT security weaknesses, we determined that IT continues to be a challenge for PBGC management. We identified five areas of concern and twenty-four recommendations. In addition to those in this report, twelve FISMA-related findings with thirty-eight recommendations were reported in our FY 2013 financial statement audit internal control report. Based on the nature of the issues identified and the continued existence of unremediated recommendations, we concluded that PBGC does not have an effective information security program.

We would again like to take this opportunity to express our appreciation for the overall cooperation that we received while performing the audit.

Attachment

cc: Patricia Kelly
Phil Langham
Alice Maroni
Ann Orr
Jioni Palmer
Sandy Rich
Judith R. Starr
Barry West
Marty Boehm

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Deborah Stover-Springer
Acting Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, N.W.
Washington DC 20005-4026

Dear Ms. Stover-Springer:

We are pleased to provide the Fiscal Year (FY) 2013 Federal Information Security Management Act (FISMA) Independent Evaluation Report, detailing the results of our review of the Pension Benefit Guaranty Corporation (PBGC) information security program.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FISMA requires Inspectors General (IG) to conduct annual evaluations of their agency's security programs and practices, and to report to Office of Management and Budget (OMB) the results of their evaluations. OMB Memorandum M-14-04, "FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management" provides instructions for completing the FISMA evaluation. Evaluations conducted by Offices of Inspector General (OIG) are intended to independently assess whether the agencies are applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions.

CliftonLarsonAllen LLP completed the required responses on behalf of the PBGC OIG. The OIG then reviewed, approved, and submitted the responses to OMB on November 22, 2013. This evaluation report provides additional information on the results of our review of the PBGC information security program.

In preparing required responses on behalf of the OIG, we coordinated with PBGC management and appreciate their cooperation in this effort. PBGC management has provided us with a response (dated March 11, 2014) to the draft FISMA 2013 Independent Evaluation Report.

The projection of any conclusions, based on our findings, to future periods is subject to the risk that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

CliftonLarsonAllen LLP

Calverton, Maryland
March 19, 2014

TABLE OF CONTENTS

Page

I. EXECUTIVE SUMMARY 1

II. BACKGROUND 1

III. OBJECTIVES 2

IV. SCOPE & METHODOLOGY 2

V. SUMMARY OF CURRENT YEAR TESTING 3

VI. FINDINGS AND RECOMMENDATIONS 4

1. Information Technology Controls for The Protection of Privacy 4
2. Plan of Action and Milestones (POA&M) 5
3. Incidence Response 6
4. Application Specific General Controls 7
5. Review of Interconnection Security Agreements 8

VII. FISMA-RELATED FINDINGS REPORTED IN THE FINANCIAL STATEMENT AUDIT 9

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2013 19

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS 19

X. MANAGEMENT RESPONSE 20

I. EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law No. 104-347), also called the Federal Information Security Management Act (FISMA), requires agencies to adopt a risk-based, life cycle approach to improving computer security that includes annual security program reviews, independent evaluations by the Inspector General (IG), and reporting to the Office of Management and Budget (OMB) and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

We are reporting five (5) FISMA findings with twenty-four (24) recommendations for Fiscal Year (FY) 2013 based on the results of our FY 2013 independent evaluation. We note that these are the total of findings and recommendations related to information technology weaknesses. In addition to those in this report, twelve (12) FISMA-related findings with thirty-eight (38) recommendations were reported in the Corporation's FY 2013 internal control report based on our FY 2013 financial statements audit work. Based on the nature of the issues identified and the continued existence of unremediated recommendations, we concluded that PBGC does not have an effective information security program.

II. BACKGROUND

The Pension Benefit Guaranty Corporation (PBGC) protects the pensions of approximately 42 million workers and retirees in more than 24 thousand private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of the Benefits Administration and Payment Department (BAPD) and information technology (IT). Internal controls over these operations are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

PBGC has become increasingly dependent on computerized information systems to execute its operations and to process, maintain, and report essential information. As a result, the reliability of computerized data and of the systems that process, maintain, and report this data is a major priority for PBGC. While the increase in computer interconnectivity has changed the way the government does business, it has also increased the risk of loss and misuse of information by unauthorized or malicious users. Protecting information systems continues to be one of the most important challenges facing government organizations today.

Through FISMA, the U.S. Congress showed its intention to enhance the management and promotion of electronic government services and processes. Its goals are to achieve more efficient government performance, increase access to government information, and increase citizen participation in government. FISMA also provides a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

PBGC operates an open and distributed computing environment to facilitate collaboration and knowledge sharing, and support its mission of protecting the pensions of over 42 million workers and retirees. It faces the challenging task of maintaining this environment, while protecting its critical information assets against malicious use and intrusion.

The PBGC Office of Inspector General (OIG) contracted with CliftonLarsonAllen LLP to conduct PBGC's FY 2013 FISMA Independent Evaluation. We performed this evaluation in conjunction with our review of information security controls required as part of the annual financial statement audit.

III. OBJECTIVES

The purposes of this evaluation were to assess the effectiveness of PBGC's information security program and practices and to determine compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

IV. SCOPE & METHODOLOGY

To perform our review of PBGC's security program, we followed a work plan based on the following guidance:

- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST Special Publication 800-37, Guide for the Security Certification and Accreditation *of Federal Information Systems,* for certification and accreditation controls.
- NIST Special Publication 800-53A*, Guide for Assessing the Security Controls in Federal Information Systems,* for the assessment of security control effectiveness.
- Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual* (FISCAM: GAO-09-232G), for information technology audit methodology.

The combination of these methodologies allowed us to meet the requirements of both FISMA and the Chief Financial Officer's Act.

Our procedures included internal and external security reviews of PBGC's information technology (IT) infrastructure; reviewing agency Plans of Action and Milestones (POA&Ms); and evaluating the following subset of PBGC's major systems:

- Consolidated Financial System (CFS)
- Pension Insurance Modeling System (PIMS)
- Electronic Complaints and Tracking System (eCATS)
- Pension and Lump Sum System (PLUS)

We performed procedures to test (1) PBGC's implementation of an entity-wide security plan, and (2) operational and technical controls specific to each application such as service continuity, logical access, and change controls. We also performed targeted tests of controls over financial and business process applications. We performed our review from April 3, 2013 to September 30, 2013 at PBGC's headquarters in Washington DC. We also performed a security assessment of the PLUS application in July 2013 at State Street Corporation in Quincy, Massachusetts.

This independent evaluation was prepared based on information available as of September 30, 2013.

V. SUMMARY OF CURRENT YEAR TESTING

Our review of IT controls covered general and selected business process application controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer systems. They include entity-wide security management, access controls, configuration management, segregation of duties and contingency planning controls. Business process application controls are those controls over the, confidentiality, integrity and availability of transactions and data during application processing.

Our review also included the integration of financial management systems to ensure effective and efficient interrelationships. These interrelationships include common data elements, common transaction processing, consistent internal controls, and transaction entry.

IT continues to be a challenge for PBGC management. The safeguarding of PBGC's systems and data is essential to protect PBGC's operations and mission. The OIG and others have consistently identified serious internal control vulnerabilities and systemic security control weaknesses in the IT environment over the last several years.

PBGC has made progress in addressing IT security weaknesses at the root-cause level by establishing the foundation for effective security controls within the National Institutes of Standards and Technology (NIST) Risk Management Framework, but these controls require time to mature and show evidence of their effectiveness. PBGC has:

- continued to lay the groundwork in the deployment of tools, acquisition of staff, and development of approaches that will enable the PBGC to better manage the design, implementation, and operational status and effectiveness of its IT security controls;
- continued to develop and implement procedures and processes for the consistent implementation of common security and configuration management controls to minimize security weaknesses; and
- improved its communication on information security progress and deficiencies to the PBGC Executive Management Committee (EMC), with briefings in February and June 2013, as part of a new process to hold PBGC more accountable to audit deadlines and inform senior management of issues, barriers, and priorities to address closure of audit findings.

In prior years, we reported that PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. PBGC has now established the foundation for implementing a more effective entity-wide security program. In 2013, PBGC issued the *IT Security Architectural Analysis Recommendations Report* that provides a blueprint for implementing entity-wide controls and addressing PBGC's security program's strengths, weaknesses, threats, and opportunities. PBGC also completed work on a long-standing weakness relating to Interconnection Security Agreements with all external organizations whose systems connect with PBGC systems. Deficiencies persisted in FY 2013, which prevented PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. While the *IT Security Architectural Analysis Report* represents progress, much remains to be done to implement and ensure adequate operation of controls. PBGC is still in the process of implementing a continuous monitoring program through the deployment and implementation of automated and manual tools, processes and procedures. PBGC acquired services from the Department of Justice to use their hosted Cyber Security Assessment and Management (CSAM) system to automate and support a consistent and effective approach to Plan of Action and Milestones (POA&M) management, the development

and maintenance of security artifacts, and the management of common controls. Migration of POA&Ms and artifacts is underway. Without a well-designed and fully implemented information security management program, there is increased risk that security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low risk resources.

Our current year audit work found deficiencies in the areas of security management, access controls, and configuration management. Control deficiencies were also found in policy administration, and the Security Assessment & Authorization (SA&A) of major applications and contractor 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 needs to continue improving and implementing a more cohesive corrective action process to address its programmatic IT weaknesses. This framework will require time for effective control processes to mature.

The financial internal control findings related to entity-wide security program planning and management, access controls and configuration management were reported in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2013 and 2012 Financial Statements Audit* (AUD-2014-2 /FA-13-93-1)[1] issued on November 15, 2013. As a result of our findings, we made recommendations to correct the deficiencies. A table summarizing these findings is in Section VII of this report.

In addition, we are reporting deficiencies in the following FISMA areas for FY 2013:

1. Information Technology Controls for The Protection of Privacy;
2. Plan of Action and Milestones (POA&M);
3. Incidence Response;
4. Application Specific General Controls; and
5. Review of Interconnection Security Agreements.

In addition, our audit also found deficiencies specifically related to responses required by OMB Memorandum M-14-04 which are included in this report. These findings and recommendations, not previously reported, are as follows.

VI. FINDINGS AND RECOMMENDATIONS

1. Information Technology Controls for The Protection of Privacy

Issues regarding the protection of sensitive information continue to exist from previous years. PBGC has not implemented controls to protect all PII in its development environment, which does not have the same level of security controls as its production systems. In FY 2013, PBGC selected a data masking solution to address PII data in non-production environments. PBGC Management indicated they plan to design and acquire the data masking solution in FY 2014.

Recommendations:

[1] http://oig.pbgc.gov/pdfs/FA-13-93-1.pdf

- Remove PII from the development environment. **(OIG Control Number FISMA-11-02)**

  PBGC's Scheduled Completion Date: 8/30/2015

In previous years, implementation of a security control baseline was not evidenced for the Corporate Data Management System (CDMS). In the past year, PBGC has combined the CDMS and the Corporate Performance Reporting System into a single authorization boundary called the Corporate Performance System (CPS). PBGC has completed the security assessment and authorization of the CPS. However, a privacy threshold analysis for CPS has not been completed and the security control matrix (SCM) that documents the planned and implemented controls for CPS were not provided for review.

Recommendations:

- Implement minimum security requirements to secure the CPS application. **(OIG Control Number FISMA-11-05)**

  PBGC's Scheduled Completion Date: 02/04/2014**

2. Plan of Action and Milestones (POA&M)

PBGC's POA&M process is not mature and ineffective. This is a longstanding issue; PBGC is still working on the process of consolidating its POA&Ms into an agency-wide POA&M. The processes are not fully developed and implemented. Since the POA&M process is still being implemented, no evidence was provided to show that the Chief Information Officer (CIO) centrally tracks, maintains and reviews/validates (independently) POA&M activities, at least, on a quarterly basis, therefore, this finding continues for FY 2013.

Recommendations:

- Develop, maintain and update PBGC's entity-wide plan of action and milestones, at least on a quarterly basis, and ensure it includes all entity-wide security deficiencies noted. **(OIG Control Number FISMA-09-08)**

  PBGC's Scheduled Completion Date: 06/15/2014

- Disseminate PBGC's entity wide POA&M to all responsible parties to ensure corrective actions are taken in accordance with POA&M. **(OIG Control Number FISMA-09-09)**

  PBGC's Scheduled Completion Date: 06/15/2014

- Ensure that the agency and program specific plan of action and milestones are tracked appropriately and provided to PBGC's CIO regularly. **(OIG Control Number FISMA-09-10)**

  PBGC's Scheduled Completion Date: 06/15/2014

- Ensure PBGC's CIO centrally tracks, maintains and independently reviews/validates POA&M activities, at least on a quarterly basis. **(OIG Control Number FISMA-09-11)**

  PBGC's Scheduled Completion Date: 06/15/2014

** PBGC submitted documentation to close this recommendation. The auditors determined that further management clarification or corrective action was needed. PBGC needs to provide a revised completion date based on the OIG's feedback.

3. Incidence Response

PBGC's Incident Response Program is inadequate and ineffective. Security and other events are first reviewed by subject matter experts (SME) to determine significance and classification. However, this evaluation process is performed by contractors with little or no oversight or review by PBGC managers. Data for trending correlation and analysis is not collected for intelligence, rapid incident response, log management, and extensible compliance reporting. Because of no federal oversight, this results in the contractor making important decisions for the government. Furthermore, PBGC's incident handling heavily relies on manual processes for analyzing and validating security events reported by its intrusion detection system. Therefore, increasing the likelihood of human error and emphasizing the need for federal oversight.

PBGC does not have or use Security Information and Event Management (SIEM) tools to enhance its ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information.[2]

Additionally, we found that PBGC's policies for safeguarding sensitive information and acceptable use of IT resources were ineffective and did not properly restrict the usage of personal e-mail to conduct PBGC business. An incident occurred in FY 2013 where an employee did not comply with PBGC's policies that govern acceptable use of information technology and protecting sensitive information. This incident involved the use of personal e-mail and employee owned equipment for business purposes. Sensitive PBGC information was compromised and placed on the Internet.

Recommendations:

- Update and document the security event categorization procedures and decision process to better define the thresholds where security events are categorized as suspicious and are recorded in a ticketing system as an incident for escalation and further analysis. **(OIG Control Number FISMA-13-01)**

- Establish a periodic review (at least quarterly) process for contractor's compliance, including the execution of PBGC's security event categorization procedures and decision process, review of Intrusion Detection System (IDS) logs, and other continuous monitoring activity. **(OIG Control Number FISMA-13-02)**

- Ensure that security incidents are documented, investigated, reported to federal management, and corrective actions implemented to remediate security vulnerabilities. **(OIG Control Number FISMA-13-03)**

- Develop factors to prioritize security incidents such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the

[2] SIEM tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components. SIEM tools can also facilitate audit record correlation and analysis.

information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident). **(OIG Control Number FISMA-13-04)**

- Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk. **(OIG Control Number FISMA-13-05)**

- Develop and Implement controls to enhance PBGC's ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information. **(OIG Control Number FISMA-13-06)**

- Review, update, and approve Directive IM 10-3, Protecting Sensitive Information. **(OIG Control Number FISMA-13-07)**

4. Application Specific General Controls

We noted the following weaknesses in the general controls designed to protect the Pension Insurance Modeling System (PIMS) application.

- A risk assessment has not been conducted for PIMS.
- PIMS is not protected by controls in the PBGC data center. The PIMS "drone farm" is physically located separately from the PBGC data center.
    - The PIMS "drone farm" does not have adequate environmental and physical security controls to protect the 47 PIMS workstations.
- PIMS does not have an established Contingency Plan in place to recover the PIMS application and database following a disruption. PBGC cannot perform modeling and make projections, if PIMS is not available.
- PIMS does not have a Continuity of Operations Plan (COOP) as PBGC has not considered PIMS a mission critical application.
    - Policy, Research and Analysis Department (PRAD) had recorded in the FY 2012 Business Impact Analysis that PIMS produces the forecasts of potential financial positions of insurance programs. However, PIMS is not listed as a required IT component.
- PIMS is not adequately supported by PBGC's general support systems and does not fully inherit common controls from these systems.
- Developers have access to the PIMS production environment.
- PRAD has not adopted and implemented PBGC's *Life Cycle Security Standard* in its maintenance of PIMS.
- Technical controls have not been implemented to separate incompatible duties in PIMS.
- A Security Assessment and Authorization (SA&A) is planned for PIMS, but has not started.

Recommendations:

- Complete a security risk assessment for PIMS. **(OIG Control Number FISMA-13-08)**

- Move the PIMS "drone farm" to the PBGC data center. **(OIG Control Number FISMA-13-09)**

- Ensure that PIMS is included in the PBGC COOP. **(OIG Control Number FISMA-13-10)**

- Develop and document a Contingency Plan for PIMS. **(OIG Control Number FISMA-13-11)**

- Ensure that PIMS is adequately supported by PBGC's general support systems and inherits common controls from these systems. **(OIG Control Number FISMA-13-12)**

- Appropriately restrict developers' access to the PIMS production environment with provisions for PBGC to allow and monitor temporary emergency access, when needed. **(OIG Control Number FISMA-13-13)**

- PRAD should adopt and implement PBGC's Life Cycle Security Standard in its maintenance of PIMS. **(OIG Control Number FISMA-13-14)**

- Develop and implement technical controls to separate incompatible duties in PIMS**. (OIG Control Number FISMA-13-15)**

- Conduct a Security Assessment and Authorization (SA&A) review process for PIMS. **(OIG Control Number FISMA-13-16**)

5. Review of Interconnection Security Agreements

PBGC's process for documenting its interconnection security agreements with other entities had outdated documents and incomplete attachments; the tracking document was also incomplete. The specific weaknesses noted were as follows:

- Three instances where the interconnecting agency's Authorization to Operate had expired;
  - Department of Commerce (DoC) National Technical Information Service (NTIS) eALG
  - Internal Revenue Service (IRS) Health Coverage Tax Credit (HCTC) Program
  - Department of Interior (DoI) Interior Business Center (IBC) Federal Payroll and Personnel System (FPPS)
- One instance where the ISA Checklist did not accurately reflect the expiration date;
  - Social Security Administration (SSA) DeathMatch; and
- One instance where the ISA was incomplete (appendices were not included).
  - Social Security Administration (SSA) DeathMatch.

Recommendations:

- Ensure the Information Security Agreement Tracking Document is reviewed for accuracy and completeness. **(OIG Control Number FISMA-13-17)**

- Review the Information Security Agreements to ensure they are current and complete. **(OIG Control Number FISMA-13-18)**

VII. FISMA-RELATED FINDINGS REPORTED IN THE FINANCIAL STATEMENT AUDIT

The following table summarizes FISMA-related findings noted under entity-wide security program planning and management, access controls, and configuration management, that were reported in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2013 and 2012 Financial Statements Audit* (AUD-2014-3 /FA-13-93-2) issued November 15, 2013.

Finding Summary	Recommendation
1. In prior years, we reported that PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. Though progress was made as highlighted below, deficiencies persisted in FY 2013, which prevented PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. PBGC has now established the foundation for implementing a more effective entity-wide security program. In 2013, PBGC issued the IT Security Architectural Analysis Recommendations Report that provides a blueprint for implementing entity-wide controls and addressing PBGC's security program's strengths, weaknesses, threats, and opportunities. PBGC also completed work on a long-standing weakness relating to Interconnection Security Agreements with all external organizations whose systems connect with PBGC systems. PBGC acquired services from the Department of Justice to use their hosted Cyber Security Assessment and Management (CSAM) system to automate and support a consistent and effective approach to Plan of Action and Milestones (POA&M) management, the development and maintenance of security artifacts, and the management of common controls. Migration of POA&Ms and artifacts is underway. While the *IT Security Architectural Analysis Report* represents progress, much remains to be done to implement and ensure adequate operation of controls. PBGC is still in the process of implementing a continuous monitoring program through the deployment and	Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses. **(OIG Control # FS-09-01) (PBGC scheduled completion date: June 30, 2013; revised date: August 31, 2015)** Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other federal agencies. **(OIG Control # FS-09-03) (PBGC scheduled completion date: September 30, 2012; revised date: August 31, 2015)** Complete the development and implementation of the redesign of PBGC's IT infrastructure; and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control # FS-09-04) (PBGC scheduled completion date: February 28, 2015; revised date: August 31, 2015)**

Finding Summary	Recommendation
implementation of automated and manual tools, processes and procedures. Without a well-designed and fully implemented information security management program, there is increased risk that security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.	
2. Security Assessments and Authorizations (SA&As) for several major applications were not completed. SA&A serves as a control to verify and validate that system security controls are properly implemented and working correctly. While a majority of SA&As have been completed by the Bureau of Public Debt through an interagency agreement with PBGC, this long standing issue is critical to complete. PBGC reported that, as a result of an updated inventory registration process, it identified several additional systems that require SA&As. The new Office of Information Technology Enterprise Information Security Authorization & Assessment Package Review Work Instructions, dated August 27, 2013, and the migration to CSAM will assist PBGC in completing the SA&A for its major applications. Less than one-half of security controls were implemented. Using NIST SP 800-53, Recommended Security Controls for Federal Information Systems, PBGC identified 208[3] common security controls. PBGC stated that 93 of these controls have been implemented. While PBGC anticipates completion of their corrective actions in early 2015, as of the end of FY 2013, they have not documented the details of the specific actions needed to complete and confirm the	Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 208 identified common security controls. **(OIG Control # FS-08-01) (PBGC scheduled completion date: February 28, 2015)** Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control # FS-09-02) (PBGC scheduled completion date: September 30, 2012; revised date: August 31, 2015)** Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC OIT operations. **(OIG Control # FS-09-07) (PBGC scheduled completion date: September 30, 2012; revised date: August 31, 2014**) Implement an effective review process to validate the completion of the SA&A packages for all major applications. The review should not be performed by an individual associated with the performance of the SA&A, or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control # FS-08-02)**

[3] PBGC updated the number of common security controls identified from 130 to 208.

Finding Summary	Recommendation
design, implementation, and operating effectiveness of the remaining 115 identified common security controls. This places PBGC at risk for insufficient protection of sensitive or critical resources or disproportionately high expenditures for common security controls. Without full development and implementation, common security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Security infrastructure design and implementation weaknesses continue. PBGC's ability to effectively implement common security controls across its systems and applications was adversely affected because there are weaknesses in its infrastructure design and deployment strategy for systems and applications. Historic weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications continued to adversely affect its ability to effectively implement common security controls across its systems and applications. Such conditions lead to inadequate protection of sensitive or critical resources or duplication of overlapping controls. Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for all needed security awareness training. PBGC will be using an automated tool, the Talent Management System, to provide security awareness and role based training.	**(PBGC scheduled completion date: June 30, 2013; revised date: TBD**)** Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the SA&A process for all major applications. **(OIG Control # FS-09-05) (PBGC scheduled completion date: September 30, 2012; revised date: TBD**)** Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the SA&A review process for major applications. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control # FS-09-06) (PBGC scheduled completion date: September 30, 2012; revised date: TBD**)** Implement an independent and effective review process to validate the completion of the SA&A packages for all major applications. **(OIG Control # FS-08-03-M-A) (PBGC scheduled completion date: June 30, 2013; revised date: August 31, 2014)** Implement a documented, independent and effective review process to validate the completion of the SA&A packages for general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control # FS-08-03-M-B) (PBGC scheduled completion date: September 30, 2012; revised date: August 31, 2014)**
3. Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for all needed security awareness training. PBGC will be using an automated tool, the Talent Management System, to provide security awareness and role based training.	Continue to disseminate the awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04) (PBGC scheduled completion date: September 30, 2012; revised date: TBD*)**

Finding Summary	Recommendation
4. Although access controls and configuration management controls are an integral part of an effective information security management program, access controls remain a systemic problem throughout PBGC. PBGC's past decentralized approach to system development, system deployments, and configuration management created an environment that lacks a cohesive structure in which to implement controls and best practices. Weaknesses in the IT environment contributed significantly to deficiencies in system configuration, segregation of duties, role□based access controls, and monitoring. PBGC realizes these challenges, and is implementing a disciplined and integrated approach through development of Configuration, Change, and Release Management (CCRM) Process and Procedures consistent with NIST SP 800-53, Rev 3. PBGC has developed and is implementing additional policies and procedures, including deploying technical and configuration management tools. PBGC is in the process of procuring, implementing and deploying technical tools to better manage configuration of common operating platforms. Once these tools are fully operational in the infrastructure, they will help ensure that controls related to the configuration of infrastructure components remain consistent and provide alerting capabilities when components are changed. Other complementary processes, such as the Patch and Vulnerability Management Group (PVMG, formerly the Tiger Team) focus on system scanning and vulnerability management, support PBGC's capability to carefully document and validate system vulnerabilities and provide evidence as to the operating effectiveness of some technical common controls. PBGC updated and improved its processes and procedures in FY 2013, including issuing the: o Infrastructure Configuration Management Plan (ICMP) on March 21, 2013;	Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control # FS-09-12) (PBGC scheduled completion date: October 31, 2013; revised date: June 15, 2015)** Develop and implement procedures and processes for the consistent implementation of common configuration management controls to minimize security weaknesses in general support systems. **(OIG Control # FS-07-07) (PBGC scheduled completion date: October 31, 2013; revised date: December 15, 2013)** Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # FS-09-13) (PBGC scheduled completion date: October 31, 2013; revised date: March 15, 2015)** Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control # FS-09-14) (PBGC scheduled completion date: October 31, 2013; revised date: March 15, 2015)** Ensure test, development, and production databases are appropriately segregated to protect sensitive information, and fully utilized to increase system performance. **(OIG Control # FS-09-15) (PBGC scheduled completion date: October 31, 2013; revised date: August 30, 2015)** Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control # FS-09-16) (PBGC scheduled completion date: October 31, 2013; revised date: August 15, 2014)**

Finding Summary	Recommendation
o Updated Configuration Management (CM) Process and Standard Operating Procedure (SOP) on March 21, 2013; o Business Change Management Process (BCMP) and SOP April 18, 2013; and o Updated Change Advisory Board (CAB) Charter on February 21, 2013.	
5. System configuration settings. Controls are not consistently applied to ensure that authentication parameters for general support systems (e.g. Novell, Windows, SUN Solaris, Oracle, etc.) and applications comply with PBGC's Information Security Policy (formerly IAH). PBGC's past decentralized approach to system development and configuration management has made it particularly difficult to implement consistent technical controls across PBGC's many systems, platforms, and applications. The failure to follow secure build standards and reassign or remove unowned user files provides internal and external attackers additional paths into PBGC's systems and could result in an increased risk of unauthorized access, modification, or deletion of sensitive system and participant information. In FY 2013, PBGC began the implementation of standards and procedures, deploying automated tools and enhanced infrastructure controls to more consistently apply authentication controls. Implementation and deployment of these controls now require time to mature in PBGC's environment, and prove their effectiveness.	Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications comply with PBGC Information Security Policy (formerly IAH). **(OIG Control # FS-07-11) (PBGC scheduled completion date: July 31, 2014)** Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control # FS-09-19) (PBGC scheduled completion date: October 31, 2013; revised date: March 15, 2015)**
6. Database configuration. Vulnerabilities found in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. These PBGC system vulnerabilities are caused by an ineffective deployment strategy in the development, test, and production environments. Ineffective system deployments have resulted in an	Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control # FS-07-14) (PBGC scheduled completion date: October 31, 2013; revised date: March 15, 2015)** Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in

Finding Summary	Recommendation
environment that is in disarray. PBGC has deployed additional technical tools to address this weakness, but requires additional cycle time to determine effectiveness. In FY 2013, PBGC updated its Configuration Management Process and SOPs to include the use of technologies to support the Configuration Verification and Audit activity. PBGC has started to replace its non-standard, End-of-Service-Life server infrastructure with standardized, secure server images. PBGC also established in FY 2013, approved baseline configurations for a majority of its production databases and networking devices. PBGC reported several accomplishments. It is beginning to use its newly acquired automated reporting capabilities to continuously monitor and address identified deviations from the established configuration baselines. Manual reporting SOPs are being implemented for cases where automation is not possible. It has begun institutionalizing the monthly review of automated and manual compliance reports to support its continuous monitoring process.	the development, test, and production environments. **(OIG Control # FS-09-20) (PBGC scheduled completion date: October 1, 2014; revised date: March 15, 2015)**
7. Segregation of duties, restriction of access to production environment. Some developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of the application, the circumvention of critical controls, and unnecessary access to sensitive data. Weaknesses in the design of PBGC's infrastructure and deployment strategy for legacy systems and applications created an environment where developers have unrestricted access to production. PBGC has identified the developers who have access to particular production assets, and removed unnecessary developer access to production. In some instances access cannot be restricted; PBGC is in the process of implementing compensating controls to restrict developer's access. PBGC has improved the process for granting access to its network and applications by updating the Network & Workspace Access, Transfer,	Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10) (PBGC scheduled completion date: December 31, 2012; revised date: January 3, 2014)**

Finding Summary	Recommendation
and Modification processes to enhance the access approval workflow. However, PBGC has not fully resolved infrastructure design issues. PBGC is in the process of implementing technical and automated controls, but these enhanced configuration controls have not matured to ensure developer's access is properly restricted. The failure to appropriately restrict privileged access to the production environment could result in unauthorized access/modification/deletion of sensitive system and/or participant information, and the release of harmful codes into the production environment.	
8. Recertification of user and system access. The OIT recertification process remains incomplete and does not include all user and system access accounts. In addition, the Recertification of User Access Process, version 4.0, does not explicitly state that all accounts (e.g. user, system, and service) across all platforms and applications will be recertified annually. PBGC's infrastructure design and configuration management weaknesses have contributed significantly to its inability to effectively implement controls to recertify all user and system accounts. The recertification process is still undergoing changes to ensure all major information systems are reviewed. In FY 2013, we noted that access account recertification packages were not complete for all systems. The account recertification for some systems did not include the approved user list, and in other systems, did not include the signed recertification letter. Unauthorized users could gain access to PBGC's data and personally identifiable information. Without periodic recertification of accounts (user, generic, service and system) management does not have adequate assurance that only current authorized users have access to PBGC resources.	Complete the implementation of the recertification process for all user and system accounts. Continue to perform annual recertification and include all PBGC's accounts (e.g. user, generic, service, and systems accounts) for general support systems and major applications. **(OIG Control # FS-07-13) (PBGC scheduled completion date: July 31, 2013; revised date: December 31, 2013)**
9. Management of user, generic and dormant accounts. PBGC's policies and practices have not effectively restricted the addition of	Continue to remove unnecessary user and generic accounts**. (OIG Control # FS-07-08) (PBGC scheduled completion date: July 31, 2012; revised**

Finding Summary	Recommendation
unnecessary generic accounts to systems in production. PBGC's configuration management weaknesses have contributed significantly to its inability to effectively implement controls to ensure the consistent removal and locking out of generic or dormant accounts. The lack of controls to remove/disable inactive accounts and dormant accounts exposes PBGC's systems to exploitation and compromise. PBGC has taken action to review generic accounts in the general support systems (GSS), removing those that are unnecessary, and approving those that are necessary. For example, PBGC introduced automated tools in its GSS to more effectively control the dormant account process. The new automated process requires time to mature to prove its effectiveness. However, more work is needed to ensure that all unnecessary and generic accounts are removed. The failure to identify and remove unnecessary accounts from the system could result in PBGC's systems being at an increased risk for unauthorized access, modification, or deletion of sensitive system and/or participant information.	**date: October 31, 2014)** Assess the risk associated with the lack of segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. **(OIG Control # FS-09-17) (PBGC scheduled completion date: February 15, 2013; revised date: August 31, 2014)** For the remaining systems, apply controls to remove/disable inactive and dormant accounts after a specified period in accordance with the PBGC Information Security Policy (formerly Information Assurance Handbook - IAH). **(OIG Control # FS-07-12) (PBGC scheduled completion date: July 31, 2012; revised date: TBD**)**
10. Audit logging and security monitoring. Periodic logging and monitoring of security related events for PBGC's applications were inadequate for the Consolidated Financial System (CFS), Premium Accounting System (PAS), Participant Records Information System Management (PRISM), and Integrated Value of Future Benefits (IPVFB) systems. PBGC's IT infrastructure consists of multiple legacy systems and applications that do not have a coherent architecture for management and security. Specific controls are not in place to ensure adequate consideration of the potential security impacts due to changes to an information system or its surrounding environment. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur, undetected. PBGC has standardized the auditable events common to all GSS infrastructure	Implement a logging and monitoring process for application security-related events and critical system modifications (e.g. CFS, PAS, TAS, PRISM, and IPVFB). **(OIG Control # FS-07-17) (PBGC scheduled completion date: April 30, 2013; revised date: August 31, 2015)**

Finding Summary	Recommendation
components. PBGC has documented and approved Audit Configuration Settings for how to configure auditable events on particular devices, including servers, databases, communications devices, etc. PBGC is currently implementing the configuration of these auditable events across all devices. A Central Audit Logging solution has been selected and procurement is in process. This solution will act as a central repository for the collection, querying and reporting functions to support PBGC's Continuous Monitoring program.	
11. Application access controls. Privileged TeamConnect group accounts use shared accounts to grant access to users. The activity by these privileged users cannot be tracked and/or traced to an individual user. Additionally, TeamConnect developers have access to both the development and production system. Malicious changes could be made without detection.	Establish unique accounts for each user in TeamConnect. (OIG Control # FS-11-02) **(PBGC scheduled completion date: September 30, 2012; revised date: TBD**)** Restrict developer's access to production. (OIG Control # FS-11-03) **(PBGC scheduled completion date: March 31, 2012; revised date: TBD*)** Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs. (OIG Control # FS-11-04) **(PBGC scheduled completion date: December 30, 2012; revised date: December 31, 2013)** Implement compensating controls for log and review of changes made by powerful shared accounts. (OIG Control # FS-11-05) **(PBGC scheduled completion date: December 31, 2012; revised date: December 31, 2013)**
12. Business process controls. The Policy, Research and Analysis Department (PRAD) uses spreadsheets in the determination of the interest rate factor used for calculating PBGC's liabilities for future benefits, that do not have adequate controls over access to data, information security and changes. A contributing factor that sets the stage for this deficiency is PRAD's lack of adequate documentation of its process and procedures to ensure that spreadsheet calculations and other activities can be repeated by unassociated officials.	Document all key processes and procedures used by PRAD in its calculations and other activities. **(OIG Control Number FS-13-03)** Document controls for managing spreadsheets to ensure their integrity and completeness. **(OIG Control Number FS-13-04)** Document and maintain an inventory of spreadsheets used by PRAD. **(OIG Control Number FS-13-05)** Develop, document and maintain processes and procedures to ensure that only current and approved versions of spreadsheets are being used by creating

Finding Summary	Recommendation
	standardized naming conventions and directory structures. **(OIG Control Number FS-13-06)** Develop, document and implement controls to consistently secure information embedded in spreadsheets, and limit access to spreadsheets to those with business needs. **(OIG Control Number FS-13-07)**

* PBGC has not established a revised completion date.

** PBGC submitted documentation to close this recommendation. The auditors determined that further management clarification or corrective action was needed. PBGC needs to provide a revised completion date based on the OIG's feedback.

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2013

OIG Control Number	Date Closed	Original Report Number
FISMA-11-01	8/14/13	EVAL-2012-9/FA-11-82-7
FISMA-11-03	4/04/13	EVAL-2012-9/FA-11-82-7
FISMA-11-04	9/13/13	EVAL-2012-9/FA-11-82-7
FISMA-12-01	7/05/13	EVAL -2013-6/FA-12-88-5
FISMA-12-02	8/27/13	EVAL -2013-6/FA-12-88-5

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

OIG Control Number	Original Report Number
Prior Year	
FISMA-09-08	AUD-2010-6/FA-09-64-6
FISMA-09-09	AUD-2010-6/FA-09-64-6
FISMA-09-10	AUD-2010-6/FA-09-64-6
FISMA-09-11	AUD-2010-6/FA-09-64-6
FISMA-11-02	EVAL-2012-9/FA-11-82-7
FISMA-11-05	EVAL-2012-9/FA-11-82-7
Current Year	
FISMA-13-01	
FISMA-13-02	
FISMA-13-03	
FISMA-13-04	
FISMA-13-05	
FISMA-13-06	
FISMA-13-07	
FISMA-13-08	
FISMA-13-09	
FISMA-13-10	
FISMA-13-11	
FISMA-13-12	
FISMA-13-13	
FISMA-13-14	
FISMA-13-15	
FISMA-13-16	
FISMA-13-17	
FISMA-13-18	

X. MANAGEMENT RESPONSE

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

Office of the Director

MAR 11 2014

To: Deborah Stover-Springer
Acting Inspector General

From: Joshua Gotbaum

Subject: Response to OIG FY 2013 Draft Report Regarding FISMA

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, dated February 24, 2014, relating to FY 2013 compliance with the Federal Information Security Management Act (FISMA).

We are in general agreement with the report's findings and recommendations. In the attachment to this report, we present our specific responses to each recommendation included in the report as well as our planned corrective actions. Addressing these recommendations in a timely manner is an important priority.

Attachment

cc: Sanford Rich, Chief of Negotiations and Restructuring
Judith Starr, General Counsel
Patricia Kelly, Chief Financial Officer
Alice Maroni, Chief Management Officer
J. Jioni Palmer, Chief of Policy and External Affairs
Barry West, Chief Information Officer
Marty Boehm, Director, Corporate Controls and Review Department

Response to OIG FY 2013 Draft Report Regarding FISMA

A. Incident Management

OIG Recommendation: Update and document the security event categorization procedures and decision process to better define the thresholds where security events are categorized as suspicious and are recorded in a ticketing system as an incident for escalation and further analysis.

PBGC Response: We agree with this recommendation. OIT will develop updated processes, procedures, and work instructions by December 31, 2014. These updates will define thresholds and alerts for security events, as well as outline high-level response plans for types of security incidents. The planned completion date is February 27, 2015.

OIG Recommendation: Establish a periodic review (at least quarterly) process for contractor's compliance including the execution of PBGC's security event categorization procedures and decision process, review of Intrusion Detection System (IDS) logs, and other continuous monitoring activity.

PBGC Response: We agree with this recommendation. The activities listed, such as review of IDS logs are within the scope of the current IT support contract and are being performed by a specific, dedicated IT security operations team. OIT will implement a review, at least quarterly, by Federal staff of contractor's execution of these activities. The review will include, but may not be limited to, sampling of actions taken, program documentation review and discussion of any resource constraints or suggested program improvements. Complete implementation of this recommendation requires the above recommendation to be implemented first, so the final implementation date for this recommendation will be February 27, 2015, although the initial establishment of the review process will begin before then.

OIG Recommendation: Ensure that security incidents are documented, investigated, reported to federal management, and corrective actions implemented to remediate security vulnerabilities.

PBGC Response: We agree with this recommendation. OIT is committed to improving its security incident management processes. OIT will develop updated processes, procedures, and work instructions by December 31, 2014, to ensure security incident reporting is incorporated into the Service Manager system and properly managed. The planned completion date is February 27, 2015.

OIG Recommendation: Develop factors to prioritize security incidents such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity, and the availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident).

PBGC Response: We agree with this recommendation. OIT is implementing this through SE-PRC-02-01, PBGC Security Incident Response Procedures. The expected completion of this recommendation is June 15, 2014.

OIG Recommendation: Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk.

PBGC Response: We agree with this recommendation. OIT plans to complete an analysis of current data loss prevention solutions deployed at PBGC, and determine if additional improvements are needed. The planned completion date is March 30, 2015.

OIG Recommendation: Develop and implement controls to enhance PBGC's ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information.

PBGC Response: We agree with this recommendation. OIT is currently implementing a product to aggregate certain network-generated event indicators to correlate disparate event indicators in a single product. The planned completion date is June 30, 2015.

OIG Recommendation: Review, update, and approve Directive IM 10-3, Protecting Sensitive Information.

PBGC Response: We agree with this recommendation. OIT has already begun the update of Directive IM 10-3. The planned completion date is July 30, 2014.

B. Application Specific General Controls

OIG Recommendation: Complete a security risk assessment for PIMS.

PBGC Response: We agree with this recommendation. PRAD is working on an IT Roadmap Implementation Plan to address this issue. The planned completion date is December 31, 2014.

OIG Recommendation: Move the PIMS "drone farm" to the PBGC data center.

PBGC Response: We agree with this recommendation. PRAD has already completed this task. The "drone farm" has been moved to the PBGC data center, and the room in which the drone farm was stored has been converted to cubicle office space. We expect to submit a recommendation completion form regarding this matter to the OIG soon.

OIG Recommendation: Ensure that PIMS is included in the PBGC COOP.

PBGC Response: PRAD does not agree that PIMS should be included in the PBGC COOP short-term recovery plan. We have agreed to reevaluate whether this is necessary in 2014 and to evaluate how to include PIMS in a longer-term disaster recovery plan.

OIG Recommendation: Develop and document a Contingency Plan for PIMS.

PBGC Response: We agree with this recommendation. PRAD is working on an IT Roadmap Implementation Plan to address this issue. The planned completion date is March 31, 2015.

OIG Recommendation: Ensure that PIMS is adequately supported by PBGC's general support systems and inherits common controls from these systems.

PBGC Response: We agree with this recommendation. PRAD is working on an IT Roadmap Implementation Plan to address this issue. The planned completion date is December 31, 2014.

OIG Recommendation: Appropriately restrict developers' access to the PIMS production environment with provisions for PBGC to allow and monitor temporary emergency access, when needed.

PBGC Response: We agree with this recommendation. PRAD has already taken the step to restrict developer access to read-only, and is considering additional steps in this area. The planned completion date is December 31, 2014.

OIG Recommendation: PRAD should adopt and implement PBGC's Life Cycle Security Standard in its maintenance of PIMS.

PBGC Response: We agree with this recommendation. PRAD is working on an IT Roadmap Implementation Plan to address this issue. The planned completion date is December 31, 2014.

OIG Recommendation: Develop and implement technical controls to separate incompatible duties in PIMS.

PBGC Response: We agree with this recommendation. PRAD has already taken steps to separate incompatible duties, and is considering additional steps in this area. The planned completion date is December 31, 2014.

OIG Recommendation: Conduct a Security Assessment and Authorization (SA&A) review process for PIMS.

PBGC Response: We agree with this recommendation. PRAD is working on an IT Roadmap Implementation Plan to address this issue. The planned completion date is December 31, 2014.

C. Review of Interconnection Security Agreements

OIG Recommendation: Ensure the Information Security Agreement Tracking Document is reviewed for accuracy and completeness.

PBGC Response: We agree with this recommendation. OIT will review tracking documents that record the results of the ISA review for accuracy and completeness. The planned completion date is July 30, 2014

OIG Recommendation: Review the Information Security Agreements to ensure they are current and complete.

PBGC Response: We agree with this recommendation. OIT will review such agreements in accordance with OIT's written work instruction. The planned completion date is July 30, 2014.

If you want to report or discuss confidentially any instance of misconduct, fraud, waste, abuse, or mismanagement, please contact the Office of Inspector General.

Telephone:
The Inspector General's HOTLINE
1-800-303-9737

The deaf or hard of hearing, dial FRS (800) 877-8339
and give the Hotline number to the relay operator.

Web:
http://oig.pbgc.gov/investigation/details.html

Or Write:
Pension Benefit Guaranty Corporation
Office of Inspector General
PO Box 34177
Washington, DC 20043-4177