Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

Fiscal Year 2011 Federal Information Security Management Act (FISMA) Independent Evaluation Report

May 11, 2012

EVAL-2012-9 / FA-11-82-7

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

May 11, 2012

To: Richard H. Macy
Chief Information Officer

From: Joseph A. Marchowsky
Assistant Inspector General for Audit

Subject: Fiscal Year 2011 Federal Information Security Management Act Independent Evaluation Report (EVAL-2012-9 / FA-11-82-7)

This memo transmits the fiscal year (FY) 2011 Federal Information Security Management Act (FISMA) independent evaluation report, detailing the results of our independent public accountants' review of the Pension Benefit Guaranty Corporation (PBGC) information security program.

As prescribed by FISMA, the PBGC Inspector General is required to conduct annual evaluations of the PBGC security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this evaluation. CliftonLarsonAllen LLP, with PBGC OIG oversight, completed the OMB-required responses that we then submitted to OMB on November 15, 2011. This evaluation report provides additional information on the results of CliftonLarsonAllen's review of the PBGC information security program.

Overall, the auditors determined that PBGC has not established an effective information security program and has not been proactive in reviewing security controls and identifying areas to strengthen this program. The attached report contains five new FISMA findings with 10 recommendations. In addition, 22 FISMA-related findings with 47 recommendations were reported in the Corporation's FY 2011 internal control report based on our FY 2011 financial statements audit (AUD-2012-2 /FA-11-82-2). Those findings and recommendations support the two information technology material weaknesses and formed, in part, the adverse opinion on internal control.

PBGC's response to the draft report indicates management's agreement with 9 of the 10 recommendations. PBGC management did not agree with one recommendation related to the eTalk application. In summary, OMB's FISMA reporting template requested that an agency report the number of "agency operational, FISMA reportable systems." PBGC included eTalk in its count, a system that that was no longer operational and experienced a catastrophic failure on July 21, 2011. PBGC management asserted that only retired/decommissioned systems should be removed from the system inventory. PBGC management further stated that a major information system or software application that is currently non-operational should still be maintained on the inventory, its POA&Ms tracked, and its security posture identified in FISMA reporting. Management agreed to update policies and procedures to better address when to officially remove a system from the FISMA inventory. CliftonLarsonAllen and OIG determined that the catastrophic failure of

eTalk was involuntary. We agree that PBGC should continue to track eTalk throughout the disposal process. Nevertheless, eTalk was not functioning at the time of OMB reporting and continues to be nonoperational today. Therefore we concluded that eTalk should not have been reported as an "operational" system.

We appreciate the overall cooperation that CliftonLarsonAllen and the OIG received while performing the audit.

Attachment

cc:

Vince Snowbarger	Alice Maroni	Marty Boehm
Laricke Blanchard	Patricia Kelly	
Ann Orr	Judith. Starr	

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Ms. Rebecca Anne Batts
Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, N.W.
Washington DC 20005-4026

Dear Ms. Batts:

We are pleased to provide the Fiscal Year (FY) 2011 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.

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-11-33, "FY 2011 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 15, 2011. 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 May 10, 2012) to the draft FISMA 2011 Independent Evaluation Report.

CliftonLarsonAllen LLP

Calverton, Maryland
May 11, 2012

TABLE OF CONTENTS

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 ten (10) recommendations for Fiscal Year (FY) 2011 based on the results of our FY 2011 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, twenty-two (22) FISMA-related findings with forty-seven (47) recommendations were reported in the Corporation's FY 2011 internal control report based on our FY 2011 financial statements audit work. Overall, we determined that the Pension Benefit Corporation (PBGC) has not established an effective information security program and has not been proactive in reviewing security controls and identifying areas to strengthen this program.

II. BACKGROUND

The Pension Benefit Guaranty Corporation (PBGC) protects the pensions of nearly 44 million workers and retirees in more than 27,000 private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), 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 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 nearly 44 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 Clifton Gunderson LLP to conduct PBGC's FY 2011 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)'s *Recommended Security Controls for Federal Information Systems – Special Publication (SP) 800-53* 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)
- Premium Accounting System (PAS)
- Pension and Lump Sum System (PLUS)
- eTalk
- TeamConnect
- Corporate Data Management System (CDMS)

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 6, 2011 to September 30, 2011 at PBGC's headquarters in Washington DC. We also performed a security assessment of the PLUS application in July 2011 at State Street Corporation in Quincy, Massachusetts.

This independent evaluation was prepared based on information available as of September 30, 2011.

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 completeness, accuracy, validity, confidentiality, 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.

The slow progress of mitigating PBGC's systemic security control weaknesses as well as the lack of an integrated financial management system posed increasing and substantial risk to PBGC's ability to carry out its mission during FY 2011. The extended time required and the lack of meaningful progress in PBGC's multi-year approach to correct previously reported deficiencies at the root cause level, introduced additional risks. These include technological obsolescence, inability to execute corrective actions, breakdown in communications and poor monitoring. As a result, PBGC's attempt to address entity-wide security management program deficiencies and systemic security control weaknesses at the root cause level had minimal effect.

PBGC's historical decentralized approach to system development and configuration management has exacerbated control weaknesses and encouraged inconsistency in implementing strong technical controls and best practices. The influx of 620 plans for over 800,000 participants from 2002-2005, contributed to PBGC's disjointed IT development and implementation strategy. The mandate to meet PBGC's mission objectives by implementing technologies to receive the influx of plans superseded proper enterprise planning and IT security controls. The result was a series of stovepipe solutions built upon unplanned and poorly integrated heterogeneous technologies with varying levels of obsolescence.

The Corporation continued its implementation of an enterprise multi-year corrective action plan (CAP) to address IT security issues at the root cause level. PBGC management realizes these weaknesses will continue to pose a threat to its environment for several years while corrective actions are being implemented. PBGC needs to implement interim corrective actions to ensure fundamental security weaknesses do not worsen as the CAP is being implemented.

PBGC performed a more rigorous and thorough assessment and authorization (A&A) process, formerly referred to as a certification and accreditation process. This process identified significant fundamental security control weaknesses for its general support systems many of which were reported in prior years' audits. These weaknesses remain unresolved. PBGC reports that the Corporation is in the process of performing A&As on its major applications.

We continued to find 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 A&As.

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 certification and accreditation 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 development and implementation of its CAP to address its programmatic IT weaknesses. This framework will require time for effective control processes to mature.

Based on our findings, we are reporting deficiencies in the following areas for FY 2011:

1. Entity-wide security program planning and management,
2. Access controls and configuration management,
3. Information Technology Controls for The Protection of Privacy,
4. Plan of Action and Milestones (POA&M),
5. Miscellaneous FISMA Controls.

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 2010 and 2011 Financial Statements Audit* (AUD-2012-2 /FA-11-82-2) issued on November 14, 2011. 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, our audit also found deficiencies specifically related to responses required by OMB Memorandum M-11-33 which are included in this report. These findings and recommendations, not previously reported, are as follows.

VI. FINDINGS AND RECOMMENDATIONS

1. Entity-wide security program planning and management

The eTalk application was listed as a major application in the FY 2011 PBGC systems inventory and reported as an "Agency operational, FISMA reportable" system in PBGC's November 15, 2011 submission to OMB. However, it was not available in PBGC's production environment; the eTalk application experienced a catastrophic incident on July 21, 2011, and was no longer operational. PBGC is currently exploring alternative solutions for a new system.

eTalk is a monitoring software/recording system that provides PBGC with the ability to monitor and evaluate calls for internal and third-party quality review. eTalk captures/records incoming participant calls from the Customer Contact Center's (CCC) 1-800 number. eTalk Qfiniti was purchased as a solution to provide internal quality review and evaluation in order to meet PBGC's performance measures goal to examine and improve the effectiveness of the customer service that PBGC provides. The eTalk system assists PBGC in meeting its strategic plan to improve the federal pension insurance program by providing exceptional customer service to its plan participants.

For FY 2011, OMB Memorandum 11-33 provided Federal agencies with instructions for reporting their compliance with FISMA and certain privacy requirements. In the OMB-mandated FISMA template, the first question in Section 1 asks each agency to summarize its system inventory; specifically:

> For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Agency operational, FISMA reportable, systems by Agency component (i.e. Bureau or Sub-Department Operating Element). [emphasis supplied]

This concept of "operational" – commonly called "availability" - is a fundamental component of information security, as defined in FISMA at 44 U.S.C. § 3542 and reiterated in the standards prescribed in the Federal Information Processing Standards Publication (FIPS Pub) 199 *Standards for Security Categorization of Federal Information and Information Systems:*

> **(1)** The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
>
> * * *
>
> **(C** availability, which means ensuring timely and reliable access to and use of information.

As of the November 15, 2011 OMB mandated reporting deadline for agency inventory, eTalk had been off-line for more than three months and remains non-operational as of the date of this report. Therefore, including eTalk in the count of operational systems for FISMA reporting was incorrect. Failure to accurately report inventory information to OMB hinders its ability to assess the implementation of security capabilities and measure their effectiveness.

Recommendation:

- PBGC should ensure that it answers and provides information to OMB as requested. **(OIG Control Number FISMA 11-01)**

Management Response

- Response: PBGC disagrees with both the finding and the recommendation. FISMA asks for information on "Operational" systems. However, PBGC believes (and OMB has validated) that this is not a short-term but a long-term meaning. We agree that retired/decommissioned systems should be removed from the system inventory. However, if a major information system or software application is currently non-operational, we believe it should still be maintained on the inventory, its POA&Ms tracked, and its security posture identified in FISMA reporting. In terms of impact of this finding, we see no harm in continuing to classify this system as part of the FISMA inventory, especially since PII data and other security risks may continue to reside in the system. Further, we believe that our reporting to FISMA was accurate and provided useful information to OMB. Nevertheless, we do see a need for our policies to better address when to officially remove a system from the FISMA inventory and we will clarify our procedures to state that this will occur upon retirement and decommissioning.

Auditor's Note

The eTalk system experienced a catastrophic failure on July 21, 2011 and PBGC was unable to reconstitute the system. This event was not a voluntary removal and did not follow an orderly decommissioning process. Accordingly, the eTalk

application was not operational at the reporting date. We agree with PBGC that the agency should continue to track the system during the remainder of the disposal process.

Major applications require certain minimum security controls, including availability (i.e. operational) as defined in FISMA at 44 U.S.C. §3542 and reiterated in the standards prescribed in the Federal Information Processing Standards Publication (FIPS Pub) 199 Standards for Security Categorization of Federal Information and Information Systems, noted in the finding. We continue to believe that eTalk should not be reported as operational.

2. Privacy

PBGC has not implemented controls to remove all PII in the development environment, and encrypt backup tapes containing PII information.

Recommendations:

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

  Management Response

  - Response: PBGC agrees. We have been discussing the best approach to this and have established a project to develop a data masking strategy to include categories of production data that need obfuscation and the selection of a data obfuscation tool. This is targeted to be completed by October 2012. From this, we plan to begin masking production data in nonproduction environments in FY 13.

- Encrypt and secure backup tapes that contain PII. **(OIG Control Number FISMA-11-03)**

  Management Response

  - Response: PBGC Agrees. As of December 31, 2011, all tape backups, excluding the legacy services of the Imaging Processing System (IPS), use Advanced Encryption Standard (AES) 256 bit encryption by way of the Symantec NetBackup software. We plan to address encryption of the IPS legacy services by June 2012.

PBGC has not taken necessary steps to protect privacy sensitive information in the Corporate Data Management System (CDMS) application. Because PBGC has not completed the security categorization of CDMS, it has not determined the minimum security requirements to be implemented for the CDMS application. PBGC also has not conducted a Privacy Impact Assessment (PIA) for the system, although CDMS contains PII. Additionally, user access recertification is not performed on a periodic basis and there is no formalized process to ensure appropriateness of access to CDMS.

Recommendations:

- Complete the security categorization of PBGC information systems. **(OIG Control Number FISMA-11-04)**

Management Response

- Response: PBGC agrees. It is essential to properly categorize PBGC's information systems in order to ensure that the proper authorization boundaries are established in support of the mission, business objectives, and the enterprise architecture; and to ensure that based on the information sensitivity, the appropriate security controls baseline (low, moderate, or high) is selected. PBGC's new information security policy, which was published in April 2012, requires that systems undergo security categorization in accordance with FIPS 199 and FIPS 200. In anticipation of this policy and following newly established OIT governance processes, OIT published SE-STD-01-13, PBGC Security Categorization Standard dated December 14,2012 that defines the requirements of system categorization. OIT published OIT Information Systems Registration Process dated November 14, 2011 that defines the steps to complete a classification and determination memo, a FIPS 199 determination, privacy threshold analysis and privacy impact assessment (if the system contains privacy data). All major information systems that were previously included in the PBGC FISMA inventory have been through the categorization process. Additionally, we now categorize all new subsystems, software applications and tools as they come into the enterprise, following this process. We are continuing to identify and categorize legacy software applications that number in the dozens to ensure that they are properly labeled as major information systems or whether they are subsystems, applications or tools that are contained within an existing major information system boundary.

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

Management Response

- Response: PBGC agrees. We have completed the FIPS-199 Categorization and Classification Determination. The Privacy Impact Assessment is completed. We plan to update the Security Plan as well as internally test security controls and complete vulnerability Scan in April. Annual Account Recertification is targeted to be complete by May, 2012. PBGC will identify an appropriate time for an independent Security Assessment and Authorization based on POA&Ms generated for the above.

- Conduct and document a Privacy Impact Assessment for CDMS. **(OIG Control Number FISMA-11-06)**

Management Response

- Response: PBGC Agrees. The Privacy Impact Assessment was completed April 3, 2012.

3. Plan of Action and Milestones (POA&M) (repeated from prior years)

PBGC is still working on the process of consolidating its POA&Ms. The process is not fully developed and implemented. PBGC management did not provide us with a copy of the entity wide POA&M. Lack of an up-to-date and consolidated POA&M could result in identified security deficiencies not being properly tracked and monitored, and thereby not remediated in a timely

manner. As part of the "Governance" Individual Corrective Action Plan (iCAP), the Chief Information Officer (CIO)'s security program and security processes are being redone with an expected completion date of Fall 2011. PBGC provided the Office of Information Technology (OIT)'s initial data call for POA&M items, which are being rolled up and consolidated in order for OIT to provide management support, oversight, and advice to the CIO and other PBGC management officials regarding residual risk posed by deficiencies in these systems. While PBGC has taken initial steps to develop a consolidated POA&M process, more work remains to be done, including developing an entity-wide POA&M. Therefore, this finding continued for FY 2011.

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)**

  Management Response

  - Response: PBGC agrees and established an Enterprise POA&M last fall. It includes all enterprise-wide security deficiencies that are not captured in system specific POA&Ms. It is updated at least quarterly. PBGC's official POA&M Process was officially approved in December, 2011.

- 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)**

  Management Response

  - Response: PBGC agrees and uses the Enterprise POA&M as a management tool with all responsible parties to track progress on remediating deficiencies.

PBGC's POA&M process is ineffective. We noted the following deficiencies in FY 2009, FY 2010 and again in FY 2011:

- No evidence that reports on the progress of security weakness remediation is being provided to the Chief Information Officer (CIO) on a regular basis.
- No evidence that the PBGC CIO centrally tracks, maintains, and independently reviews/validates POA&M activities on at least a quarterly basis.

PBGC Management has started the process of consolidating POA&Ms for PBGC systems, educating system owners on the POA&M process and collecting items needed to manage the process; however, management has not completed the process, including CIO reviews. According to the PBGC Corrective Action Plan, the CIO's security program and security processes are being redone with an expected completion date of Fall 2011. While PBGC has implemented additional processes in FY 2011, such as implementing a process to develop an entitywide POA&M, other POA&M process improvements related to consolidating POA&Ms across PBGC are not complete as of August 2011, and therefore were not available for review during this audit period. This finding continued for FY 2011.

Recommendations:

- 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)**

  Management Response

  - Response: PBGC agrees. The official procedures were approved in December, 2011 and are in the process of being implemented across all major systems and should be fully implemented by July 2012.

- 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)**

  Management Response

  - Response: PBGC agrees. Official POA&M procedures were approved in December, 2011 and POA&Ms are currently consolidated and presented to the CIO at least four times each year. We are targeting April 2012 to have all POA&Ms converted to the standard format from the legacy formats that have been used.

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 2011 and 2010 Financial Statements Audit* (AUD-2012-2 /FA-11-82-2) issued November 14, 2011.

Finding Summary	Recommendation
1. Weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications adversely affected its ability to effectively implement common security controls across its systems and applications. Without full development and implementation, security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions lead to insufficient protection of sensitive or critical resources or disproportionately high expenditures for controls.	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 Number FS-09-01)** Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 130 identified common security controls. **(OIG Control # FS-08-01 *Modified)** 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 Number FS-09-02)**
2. PBGC continued the implementation of its CAP to address fundamental weaknesses in its entity-wide security program planning and management. During FY 2011, PBGC began the implementation of a more rigorous and thorough A&A process. Through this process, PBGC identified significant fundamental security control weaknesses for its general support systems, many of which were reported on in prior years' audits. While this is an important step in the planning process, these security control weaknesses remain unresolved and PBGC's efforts lack sufficient meaningful and incremental progress. PBGC reports that they are in the process of performing A&As on its major applications. The slow rate of progress has introduced additional risks including technological obsolescence, inability to execute corrective actions, breakdown in communications and poor monitoring.	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 Number FS-09-03)** 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 Number FS-09-04)** Implement an effective review process to validate the completion of the A&A packages for all major applications. The review should not be performed by an individual associated with the performance of the A&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

Finding Summary	Recommendation
	the results obtained. **(OIG Control # FS-08-02 *Modified)** Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the A&A process for all major applications. **(OIG Control # FS-09-05 *Modified)** Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the A&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 *Modified)** 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 Office of IT (OIT) operations. **(OIG Control Number FS-09-07)** Implement an independent and effective review process to validate the completion of the A&A packages for all major applications. **(OIG Control # FS-08-03 *Modified)** Implement an independent and effective review process to validate the completion of the A&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 *Modified)**
3. 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. The process is ineffective and limits PBGC's ability to ensure that all required personnel have completed security awareness training.	Continue to disseminate the awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04 *Modified)**

Finding Summary	Recommendation
4. In FY 2010, PBGC's benefit payments service provider (service provider) implemented a security operations center (SOC) outside of the United States (US), without providing PBGC adequate advance notice. In FY 2011, PBGC completed a risk assessment, but it did not contain adequate evidence to verify and validate the technical security risks of the SOC. Because the SOC has some responsibility for monitoring security-related events associated with the PLUS application and components of its system boundary, it is important PBGC assess risks to its systems and implement mitigating controls to ensure compliance with PBGC's policies and procedures.	Develop and implement an immediate plan of action to address the potential security risk posed by locating the SOC outside of the US. **(OIG Control # FS-10-01)** Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and the Federal Information Security Management Act (FISMA). **(OIG Control #FS-10-02)** Ensure that adequate controls in the design and implementation of the SOC are in place to protect PBGC PLUS. **(OIG Control Number # FS-11-01)**
5. PBGC has not executed interconnection security agreements (ISA) or memorandums of understanding (MOU) between all external organizations whose systems interconnect with PBGC's systems. Controls to require such agreements do not exist. PBGC is in the process of planning and documenting security agreements for interconnection with all external organizations' systems. In the absence of an ISA and MOU, either party (PBGC or external system owner) may be unfamiliar with the technical requirements of the interconnection and the details that may be required to provide overall security for systems that are interconnected.	Develop controls and implement an ISA and MOU with all external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03 *Modified)**
6. 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. Configuration management controls are therefore not consistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server	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 Number FS-07-07)** 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 Number FS-09-12)**

Finding Summary	Recommendation
configurations; therefore, management cannot rely on results obtained in the development or test environments prior to deployment in production. Overall, the PBGC environment suffers from inadequate configuration, roles, privileges, logging, monitoring, file permissions, and operating system access.	Establish baseline configuration standards for all of PBGC's systems. **(OIG Control Number FS-09-13)** 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 Number FS-09-14)** Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance. (**OIG Control Number FS-09-15**) 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 Number FS-09-16**)
7. PBGC's policies and practices have not effectively restricted the addition of unnecessary and generic accounts to systems in production. Consequently, the number of unnecessary and generic accounts grew over the years. PBGC management has not determined if the removal of all legacy generic accounts would disrupt production activities.	Continue to remove unnecessary user and/or generic accounts. **(OIG Control Number FS-07-08)**
8. Controls are not consistently implemented to appropriately segregate duties and grant rights and privileges commensurate with the 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.	Consistently implement controls to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. **(OIG Control Number FS-07-09)** 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 *Modified)**
9. Some developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of the application, the	Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control Number FS-07-10)**

Finding Summary	Recommendation
circumvention of critical controls, and unnecessary access to sensitive data.	Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege." If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed. **(OIG Control Number FS-09-18)**
10. 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 the Information Assurance Handbook (IAH). PBGC's 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.	Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications are in compliance with the IAH. **(OIG Control Number FS-07-11)** Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control Number FS-09-19)**
11. 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.	For the remaining systems, apply controls to remove/disable inactive and dormant accounts after a specified period in accordance with the IAH. **(OIG Control # FS-07- 12 *Modified)**
12. The OIT recertification process is incomplete and only addresses generic and service accounts; it does not include all user and system 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 re-certified 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.	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 Number FS-07-13)**

Finding Summary	Recommendation
13. 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 environment that is in disarray. Security control weaknesses and vulnerabilities in key databases remain unresolved. These control weaknesses are scheduled to be corrected in 2013. These weaknesses expose PBGC to increased risk of data modification or deletion. Unauthorized changes could occur and not be detected.	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 Number FS-07-14)** Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control Number FS-09-20)**
14. Access request authorizations were not appropriately documented. PBGC has not fully implemented controls to ensure Enterprise Local Area Network (ELAN) forms are properly documented and maintained.	Ensure that adequate documentation of access authorization is maintained by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control Number FS-07-15)**
15. PBGC lacks an effective process to track contractors throughout their employment at PBGC, including appropriate notifications of start dates and separation. PBGC updated its directive PM 05-1, PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees, in FY 2011 to provide for the effective enforcement of controls designed to track entrance and separation of all Federal and contract employees. However, the implementation PM 05-1 has not reached a level of maturity to test and validate the effectiveness of these controls.	Update and enforce directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. **(OIG Control Number FS-07-16)**
16. Periodic logging and monitoring of security-related events for PBGC's applications were inadequate Consolidated Financial Systems (CFS), Premium Accounting System (PAS), Trust Accounting System (TAS), Participant Records Information Systems Management (PRISM), and Integrated Present Value of Future Benefits (IPVFB) systems. PBGC's IT 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 Number FS-07-17)**

Finding Summary	Recommendation
consists of multiple legacy systems and applications (e.g. PAS, TAS, IPVFB, PRISM, etc.) that do not have a coherent architecture for management and security.	
17. The application virtualization/application delivery product Citrix MetaFrame Presentation Server used by PBGC's benefit payments service provider to connect to its benefit payments system, PLUS, reached its end of life date on December 31, 2009. PBGC did not include the Citrix MetaFrame Presentation Server in the system boundary when conducting the A&A of the PLUS application.	Replace the Citrix MetaFrame presentation server. **(OIG Control #FS-10-04)** Include the application virtualization/application delivery product used by the benefit payments service provider to access the PLUS application in the system boundary. **(OIG Control # FS-10-05)**
18. 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.	Establish unique accounts for each user in TeamConnect. **(OIG Control Number FS-11-02)** Restrict developer's access to production. **(OIG Control Number FS-11-03)** Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs. **(OIG Control Number FS-11-04)** Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control Number FS-11-05)**
19. An MOU between PBGC and the service provider for the PLUS application was executed within PBGC between PBGC federal employees and not with the service provider. This MOU is needed to document the service provider's responsibilities and security requirements for PLUS, however, it serves no purpose since the service provider did not sign it. Further, executing the MOU between federal employees and omitting the service provider demonstrates a lack of understanding of the purpose and importance of the agreement.	Obtain a contract system representative signature on the PLUS MOU or alternatively, develop an interconnection security agreement (ISA) between PBGC and the benefit payments service provider for the connection. **(OIG Control Number FS-11-13)**
20. PBGC did not review the service provider personnel's access to the PLUS system to ensure the personnel were appropriately recertified. PBGC relies upon the service	Annually review contractor access recertifications for the benefit payments service provider employees with access to PLUS. **(OIG Control Number FS-11-14)**

Finding Summary	Recommendation
provider to test recertification and to assert that individuals have the proper access to the system. PBGC performed no further review to test the service provider's assertion that user access is appropriate. The risk to PBGC is increased as the service provider's PLUS users typically have greater access to the PLUS system than users at PBGC.	
21. PBGC did not conduct a review of the PLUS System Contingency Plan until July 2011 when we requested the documentation as part of the financial statement audit. Even after receipt of the document, PBGC did not evaluate the scope of the contingency plan nor did PBGC assess the plan's compliance with NIST SP 800-34 requirements.	Review the PLUS contingency plan for compliance with NIST SP 800-34 requirements. **(OIG Control Number FS-11-15)**
22. Our assessment of the information PBGC provided as support for assessing the risk of operating a SOC in a foreign country found that PBGC's risk assessment was not adequate. Information relied upon included a generic overview of connectivity which did not demonstrate specifics on encryption end points, protocol filters, source and destination filters and intervening infrastructure component locations critical to the analysis of any design investigations. Further, PBGC did not address the verification of background checks for the employees of the foreign country SOC and PBGC was unable to adequately assess the risks of the SOC implementation.	Develop and implement a policy to identify and document the risks associated with PBGC operations performed in foreign countries, ensure appropriate management review, and take appropriate actions to mitigate identified risks. **(OIG Control Number # FS-11-16)** For the PLUS SOC operating in a foreign country revise the existing risk assessment to identify and document risks, and take appropriate actions. **(OIG Control Number # FS-11-17)**

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2011

OIG Control Number	Date Closed	Original Report Number
FISMA-10-01	October 5, 2011	EVAL 2011-9/FA-10-69-8
FISMA-09-07	October 5, 2011	AUD-2010-6/FA-09-64-6
FISMA-09-12	October 5, 2011	AUD-2010-6/FA-09-64-6

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
Current Year	
FISMA-11-01	
FISMA-11-02	
FISMA-11-03	
FISMA-11-04	
FISMA-11-05	
FISMA-11-06	

X. MANAGEMENT RESPONSE

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

May 10, 2012

TO: Joseph A. Marchowsky
Assistant Inspector General for Audit

FROM: Richard H. Macy
Chief Information Officer

SUBJECT: Fiscal Year 2011 Federal Information Security Management Act Independent Evaluation Report (EVAL-2012-9 / FA-11-82-7) – Management Response

I am pleased to transmit the Management Response to the fiscal year (FY) 2011 Federal Information Security Management Act (FISMA) independent evaluation report, detailing the results of the independent public accountants' review of the Pension Benefit Guaranty Corporation (PBGC) Information Security Program.

The Office of Information Technology agrees fully with each of the report's recommendations, except for the report's first recommendation. We would welcome further discussion of this recommendation. We are pleased to report that we have already made progress on addressing many of the recommendations with many expected to be completely implemented this summer.

We would like to take this opportunity to express our appreciation for the overall cooperation that CliftonLarsonAllen and the OIG has provided to OIT while the review was being performed and in follow-up afterward.

Here are the specific responses to each recommendation:

Recommendation: PBGC should ensure that it answers and provides information to OMB as requested. **(OIG Control Number FISMA 11-XX) NFR#12**

> **Response:** PBGC disagrees with both the finding and the recommendation as we believe we did answer and provide information to OMB as requested. FISMA does ask for information on "Operational" systems. However, "Operational" can have many meanings including systems related to operations. In checking with OMB, we received direction that systems should not be taken off the FISMA inventory until they are retired/decommissioned. We will update our procedures to clearly indicate when systems will come off the inventory.

1

Recommendation: Remove PII from the development environment. **(OIG Control Number FISMA-11-XX) NFR #38**

Response: PBGC agrees. We have been discussing the best approach to this and have established a project to develop a data masking strategy to include categories of production data that need obfuscation and the selection of a data obfuscation tool. This is targeted to be completed by October 2012. From this, we plan to begin masking production data in non-production environments in FY13.

Recommendation: Encrypt and secure backup tapes that contain PII. **(OIG Control Number FISMA-11-XX) NFR #38**

Response: PBGC Agrees. As of December 31, 2011, all tape backups, excluding the legacy services of the Imaging Processing System (IPS), use Advanced Encryption Standard (AES) 256 bit encryption by way of the Symantec NetBackup software. We plan to address encryption of the IPS legacy services by June 2012.

Recommendation: Complete the security categorization of PBGC information systems. **(OIG Control Number FISMA-11-XX) NFR #24**

Response: PBGC agrees. It is essential to properly categorize PBGC's information systems in order to ensure that the proper authorization boundaries are established in support of the mission, business objectives, and the enterprise architecture; and to ensure that based on the information sensitivity, the appropriate security controls baseline (low, moderate, or high) is selected. PBGC's new information security policy, which was published in April 2012, requires that systems undergo security categorization in accordance with FIPS 199 and FIPS 200. In anticipation of this policy and following newly established OIT governance processes, OIT published SE-STD-01-13, PBGC Security Categorization Standard dated December 14, 2012 that defines the requirements of system categorization. OIT published OIT Information Systems Registration Process dated November 14, 2011 that defines the steps to complete a classification and determination memo, a FIPS 199 determination, privacy threshold analysis and privacy impact assessment (if the system contains privacy data). All major information systems that were previously included in the PBGC FISMA inventory have been through the categorization process. Additionally, we now categorize all new subsystems, software applications and tools as they come into the enterprise, following this process. We are continuing to identify and categorize legacy software applications that number in the dozens to ensure that they are properly labeled as major information systems or whether they are subsystems, applications or tools that are contained within an existing major information system boundary.

Recommendation: Implement minimum security requirements to secure the CDMS application. **(OIG Control Number FISMA-11-XX) NFR #24**

Response: PBGC agrees. We have completed the FIPS-199 Categorization and Classification Determination. The Privacy Impact Assessment is completed. We plan to update the Security Plan as well as internally test security controls and complete vulnerability Scan in April. Annual Account Recertification is targeted to be complete by May, 2012. PBGC will identify an appropriate time for an independent Security Assessment and Authorization based on POA&Ms generated for the above.

Recommendation: Conduct and document a Privacy Impact Assessment for CIDMS. **(OIG Control Number FISMA-11-XX) NFR #24**

Response: PBGC Agrees. The Privacy Impact Assessment was completed April 3, 2012.

Recommendation: 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) NFR #39**

Response: PBGC agrees and established an Enterprise POA&M last fall. It includes all enterprise-wide security deficiencies that are not captured in system specific POA&Ms. It is updated at least quarterly. PBGC's official POA&M Process was officially approved in December, 2011.

Recommendation: 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) NFR #39**

Response: PBGC agrees and uses the Enterprise POA&M as a management tool with all responsible parties to track progress on remediating deficiencies.

Recommendation: 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) NFR #20**

Response: PBGC agrees. The official procedures were approved in December, 2011 and are in the process of being implemented across all major systems and should be fully implemented by July 2012.

Recommendation: 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)**

Response: PBGC agrees. Official POA&M procedures were approved in December, 2011 and POA&Ms are currently consolidated and presented to the CIO at least four times each year. We are targeting April 2012 to have all POA&Ms converted to the standard format from the legacy formats that have been used.

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