Pension Benefit Guaranty Corporation

Office of Inspector General

AUDIT REPORT

Fiscal Year 2012 Federal Information Security Management Act (FISMA) Independent Evaluation Report

May 1, 2013

Eval -2013-6/FA-12-88-5

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

May 1, 2013

To: Josh Gotbaum
Director

From: Candace Milbry Candace A. Mils
Acting Assistant Inspector General for Audit

Subject: Fiscal Year 2012 Federal Information Security Management Act
Independent Evaluation Report (Eval 2013-06/FA-12-88-5)

I am pleased to transmit the fiscal year (FY) 2012 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. This is the sixth report related to the fiscal year 2012 financial statements audit (AUD-2013-1/FA-12-88-1).

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, on behalf of the PBGC OIG, completed the OMB-required responses that we then submitted to OMB on November 15, 2012. This evaluation report provides additional information on the results of CliftonLarsonAllen's review of the PBGC information security program.

Overall, the auditors determined that Information Technology (IT) continues to be a challenge for PBGC. 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's delayed progress in mitigating these deficiencies at the root-cause level continued to pose increasing and substantial risks to PBGC's ability to carry out its mission during FY 2012. Due to the persistent nature and extended time required to mitigate such vulnerabilities, additional risks threaten PBGC's ability to safeguard its systems. These risks include technological obsolescence, inability to execute corrective actions, breakdown in communications, and poor monitoring. PBGC has made some progress in addressing IT security weaknesses at the root-cause level by continuing the implementation of its FY 2010 Enterprise Corrective Action Plan (CAP), and introducing additional reporting controls to track progress.

The response to a draft of this report indicates PBGC's agreement with all recommendations and documents expected completion dates. We would again like to take this opportunity to express our appreciation for the overall cooperation that CliftonLarsonAllen and the OIG received while performing the audit.

Attachment

cc: Judith R. Starr
Patricia Kelly
Alice Maroni
Barry West
Martin O. Boehm
Ann Orr

CliftonLarsonAllen

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) 2012 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-12-20, "FY 2012 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, 2012. 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 April 24, 2013) to the draft FISMA 2012 Independent Evaluation Report.

CliftonLarsonAllen LLP

Calverton, Maryland
April 24, 2013

Page

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 two (2) FISMA findings with ten (10) recommendations for Fiscal Year (FY) 2012 based on the results of our FY 2012 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, thirteen (13) FISMA-related findings with thirty-four (34) recommendations were reported in the Corporation's FY 2012 internal control report based on our FY 2012 financial statements audit work. Based on the number of unremediated outstanding recommendations, PBGC does not have an effective information security program.

II. BACKGROUND

The Pension Benefit Guaranty Corporation (PBGC) protects the pensions of approximately 43 million workers and retirees in more than 25 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 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 CliftonLarsonAllen LLP to conduct PBGC's FY 2012 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)
- Integrated Present Value of Future Benefits (IPVFB)
- Legal Management System (LMS)
- 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 6, 2012 to September 30, 2012 at PBGC's headquarters in Washington DC. We also performed a security assessment of the PLUS application in July 2012 at State Street Corporation in Quincy, Massachusetts.

This independent evaluation was prepared based on information available as of September 30, 2012.

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 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's delayed progress in mitigating these deficiencies at the root-cause level continued to pose increasing and substantial risks to PBGC's ability to carry out its mission during FY 2012. Due to the persistent nature and extended time required to mitigate such vulnerabilities, additional risks threaten PBGC's ability to safeguard its systems. These risks include technological obsolescence, inability to execute corrective actions, breakdown in communications, and poor monitoring.

PBGC has made some progress in addressing IT security weaknesses at the root-cause level by continuing the implementation of its FY 2010 Enterprise Corrective Action Plan (CAP), and introducing additional reporting controls to track progress. Additional tracking controls include the Enterprise Plan of Action and Milestones (POA&M) and the Progress Status Reports (PSR) on corrective actions. However, the current PBGC corrective action process remains disjointed, with stove-piped responsibilities that did not provide a holistic view to inform key decision makers on progress made and resources needed to complete critical tasks. PBGC is in the process of improving its corrective action process to be more cohesive where the CAP will inform the POA&M which will, in turn, provide the Contracts and Control Review Department (CCRD) with the official status of corrective actions to be included in the Listing of Open OIG Recommendations.

The Corporation has also made progress in addressing the design of its infrastructure, account management, enterprise security management, and configuration management, but the control processes have not reached a level of maturity to prove their effectiveness. PBGC is implementing a disciplined and integrated approach to its Configuration, Change, and Release Management (CCRM) process and procedures consistent with NIST SP 800-53, Rev 3. The Corporation has also developed and is implementing additional policies and procedures; additional technical and configuration management tools are also being deployed. However, much remains to be done, and the pace of progress remains slow.

PBGC anticipated completing the assessment and authorization (A&A) process, formerly referred to as a certification and accreditation process, on the Corporation's major applications in FY 2012, but was unable to complete the process. The work on the A&As that has been performed through FY 2012 identified significant fundamental security control weaknesses in PBGC's general support systems, many of which were reported in prior years' audits and remain unresolved. 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 completion of A&As for all major applications.

PBGC developed an information security policy framework, including the Information Security Policy which is supported by standards, processes, procedures, and a guide published in June 2012, The Office of Information Technology (OIT) Security Authorization Guide. This Guide provides steps and templates for use in preparing and completing the Security Authorization and Assessment process which follows National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. Also, the Guide provides a checklist to support OIT's review of submitted artifacts as evidence of controls implemented. PBGC is documenting the review process with the checklist. The new information security policy framework has not reached a level of maturity to determine its effectiveness. PBGC is still in the process of establishing an enterprise-wide continuous monitoring program; and deploying additional network management, monitoring and configuration tools in its environment.

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 A&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 2012 and 2011 Financial Statements Audit* (AUD-2013-2 /FA-12-88-2)[1] issued on November 15, 2012. 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 2012:

1. Information Technology Controls for The Protection of Privacy,
2. Plan of Action and Milestones (POA&M).

In addition, our audit also found deficiencies specifically related to responses required by OMB Memorandum M-12-20 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

The configuration of one of PBGC's remote terminal servers allowed all PBGC remote access users, employees and contractors, read and write access to the server's local storage drive. The inadequate configuration resulted in users saving sensitive information to the drive and allowing other users (remote access PBGC employees and contractors) access to that information.

[1] http://oig.pbgc.gov/pdfs/FA-12-88-2.pdf

Information discovered on the local storage drive included participant Privacy Act data, i.e., personally identifiable information (PII)[2].

Recommendations:

- Immediately restrict access to the local storage drive on the remote terminal server so that only authorized users may read and write to the drive. **(OIG Control Number FISMA-12-01)**

  Management Response

  In FY2012 when this vulnerability was identified, OIT immediately reviewed and initiated actions to restrict access capabilities to the identified remote terminal server. OIT will provide evidence that this vulnerability no longer exists by June 30, 2013. We will then prepare and submit a Recommendation Completion Form for this item.

- Review all servers which permit remote access and validate that permissions to the local drive are configured in accordance with the concept of least privilege. **(OIG Control Number FISMA-12-02)**

  Management Response

  Based on the scope of actions executed to remediate FISMA 12-01, OIT will need time to complete the confirmation of our restricting least privilege remote access to all servers. While we plan to take action during FY 2013, we expect that we will need several months to collect the evidence to demonstrate we have installed and are following the installed solution. This places the expected timeframe to submit a Recommendation Completion Form on this by December 31, 2013.

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. Furthermore, backup tapes also have PII, but have not been encrypted to protect data from unauthorized disclosure.

Recommendations:

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

  PBGC's Scheduled Completion Date 6/30/2014:

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

  PBGC's Scheduled Completion Date 06/30/2013:

[2] Personally identifiable information (PII) is any information about an individual that is maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (based on General Accountability Office and Office of Management and Budget definitions).

PBGC has not completed the security categorization of all of its information systems.

Recommendations:

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

  PBGC's Scheduled Completion Date 12/31/2012:

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

  PBGC's Scheduled Completion Date 08/31/2013:

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

PBGC is still working on the process of consolidating its POA&Ms into an agency-wide POA&M. The process is not fully developed and implemented. In the spring of 2012, the new process was initiated, which includes having the Information System Security Officers (ISSOs) work with the Information System Owners (ISOs) to ensure that POA&M submissions are uniform. The PBGC Plan of Action and Milestones Process has a template with the required and optional fields and related definitions. These new submissions are being uploaded to the new PBGC POA&M database. The new process requires Information System/Information Owners to submit POA&M updates quarterly and the Senior Agency Information Security Officer (SAISO) is required to prepare an agency-level report for the Chief Information Officer (CIO). After the 1Q 2012 POA&M data call, the Enterprise Information Security Office prepared the Plan of Action & Milestones Quarterly Analysis FY 2012 – 1st Quarter, March 2012. Since the POA&M is a new process, and still being implemented, no evidence was provided to show that the CIO centrally tracks, maintains and reviews/validates (independently) POA&M activities, at least, on a quarterly basis, this finding continues for FY 2012.

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 12/31/2012:

- 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 12/31/2012:

PBGC's POA&M process is not mature and effective. We noted the following deficiencies in FY 2009, FY 2010, FY 2011, and again in FY 2012:

- 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.

In FY 2012, PBGC created the “PBGC Plan of Action and Milestone Process” noted above, however, the implementation of the new process has not reached a level of maturity to determine its effectiveness.

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)**

  PBGC’s Scheduled Completion Date 12/31/2012:

- 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)**

  PBGC’s Scheduled Completion Date12/31/2012:

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 2012 and 2011 Financial Statements Audit* (AUD-2013-2 /FA-12-88-2) issued November 15, 2012.

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. PBGC realizes these challenges, and has identified and documented the enterprise common security controls in the Agency Security Controls General Support System (ASCGSS) System Security Plan. PBGC completed and approved the Infrastructure Configuration Management Plan in FY 2012. The Corporation also approved its CCRM process and procedures in FY 2012. The future implementation of these strategies is designed to enable PBGC to implement a disciplined and integrated approach to CCRM, eliminate inconsistencies and weaknesses in the implementation of the processes and procedures and ensure compliance with the NIST SP 800-53, Rev 3 common controls. However PBGC had not completed and confirmed the implementation, and operating effectiveness of its common security controls; management cannot have confidence that the controls were implemented.	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)** 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) (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)**
2. PBGC had not completed A&As for any major applications. However, PBGC continued to improve the PBGC Enterprise Information Security Program which includes	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

Finding Summary	Recommendation
strengthening the system authorization process, verifying contractor A&A deliverables, and ensuring their quality and conformance to the statement of work as well as to the objectives of the PBGC risk management process and NIST SP 800-53. PBGC has focused on updating the underlying policies, strengthening the security program overall, obtaining quality contractors to conduct the assessments, and ensuring PBGC prepare for and begin the execution of the system authorization process.	those managed by contractors or other federal agencies. **(OIG Control # FS-09-03) (PBGC scheduled completion date: September 30, 2012)** 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)** 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 the results obtained. **(OIG Control # FS-08-02) (PBGC scheduled completion date: June 30, 2013)** 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) (PBGC scheduled completion date: September 30, 2012)** 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) (PBGC scheduled completion date: September 30, 2012)** 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)** Implement an independent and effective review process to validate the completion of the A&A

Finding Summary	Recommendation
	packages for all major applications. **(OIG Control # FS-08-03) (PBGC scheduled completion date: June 30, 2013)** Implement a documented, 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) (PBGC scheduled completion date: September 30, 2012)**
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 published SE-PRC-01-01, Security Awareness and Training Procedures, in June 2012. It defines both annual security awareness requirements and role-based requirements. Security incident response training is still in development and will be delivered during FY 2013 for all staff involved in security incident management and response. PBGC is in its second year of providing an online information security awareness module supplied by an OMB-approved Information System Security Line of Business provider (OPM's Go Learn Learning Management System platform). This enables more efficient tracking of staff and contractors who have taken the module. PBGC fulfilled last year's requirement for general security awareness training using this service. Role-based training for security is still in the development stage. Lack of security awareness can lead to increased risk of security breaches and exposure to fraud. Controls may not be placed in operation as mandated by PBGC policies.	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)**
4. 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	Develop controls and implement an ISA or MOU with all external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03) (PBGC scheduled completion date: September 30, 2012)**

Finding Summary	Recommendation
agreements do not exist. PBGC is in the process of planning and documenting ISAs 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.	
5. 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 inconsistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server 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.	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)** 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)** Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # FS-09-13) (PBGC scheduled completion date: October 31, 2013)** 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)** 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)** 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

Finding Summary	Recommendation
	implemented. **(OIG Control # FS-09-16) (PBGC scheduled completion date: October 31, 2013)**
6. 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. Furthermore, 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. PBGC has made progress in the recertification and dormant Account Process. However, not all major systems have gone through the recertification process such as those in the Benefits Administration and Payment Department. Furthermore, the actual removal of dormant accounts from systems is still a manual process and remains a risk to the timeliness of effective removal. 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 system, removing those that are unnecessary, and approving those that are necessary; however, more work is needed to ensure that all unnecessary and generic accounts are removed. 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.	Continue to remove unnecessary user and generic accounts. **(OIG Control # FS-07-08) (PBGC scheduled completion date: July 31, 2012)** 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)** 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) (PBGC scheduled completion date: July 31, 2012)**
7. 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	Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10) (PBGC scheduled completion date: December 31, 2012)**

	Finding Summary	Recommendation
	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. Service Desk tickets were submitted to re-establish necessary developer access along with associated necessary Risk Acceptance forms. The Corporation now has mechanisms in place within the automated Enterprise Local Area Network (eLAN) process and records to document development team members' access. There is now a better understanding of risks associated with developers' access to production to ensure access is evaluated before granting. All developers' access to production has not been eliminated; PBGC is in the process of implementing compensating controls to restrict developer's access to production. However, PBGC has not fully resolved infrastructure design issues. In the interim, PBGC implemented ACLs that will act as static firewalls until the comprehensive solution is fully implemented.	
8.	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 comply with the 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)**
9.	The OIT recertification process remains incomplete and 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 recertified annually. PBGC's infrastructure design and configuration management	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)**

	Finding Summary	Recommendation
	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. PBGC implemented an automated eLAN workflow process at the end of FY 2011, which provided another way for PBGC's customers to interact with the Service Desk and submit network and application services (eLAN) access requests. Effective May 1, 2012, PBGC required that users discontinue submitting paper eLAN forms and instead use the automated system, except in situations where the automated system does not accommodate a user's unique and specific access request due to services and functions that aren't available in PBGC's current Service Catalog. In those cases, the Service Desk is prepared to assist the user with the completion of the paper eLAN until the automated system can be modified. Current plans are to incorporate additional workflow modifications, to eliminate the need for any paper forms, into a planned Service Manager, version 7 to version 9 migration which is scheduled for FY 2013.	
10.	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. PBGC has deployed additional technical tools to address this weakness, but requires additional cycle time to determine effectiveness. 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.	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)** Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control # FS-09-20) (PBGC scheduled completion date: October 1, 2014)**

Finding Summary	Recommendation
Unauthorized changes could occur and not be detected.	
11. Periodic logging and monitoring of security-related events for PBGC's applications were inadequate for 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 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.	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)**
12. The application virtualization/application delivery product used by PBGC's benefit payments service provider to connect to its benefit payments system, PLUS, is not included in the system boundary when conducting the A&A for the PLUS application. There is no documented security plan, risk assessment, security controls testing and continuous monitoring program for the application virtualization/application delivery product.	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) (PBGC scheduled completion date: TBD)**
13. 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: TBD)** Restrict developer's access to production. (OIG Control # FS-11-03) **(PBGC scheduled completion date: September 30, 2012)** 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: TBD)** Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control # FS-11-05) (PBGC scheduled completion date: TBD)**

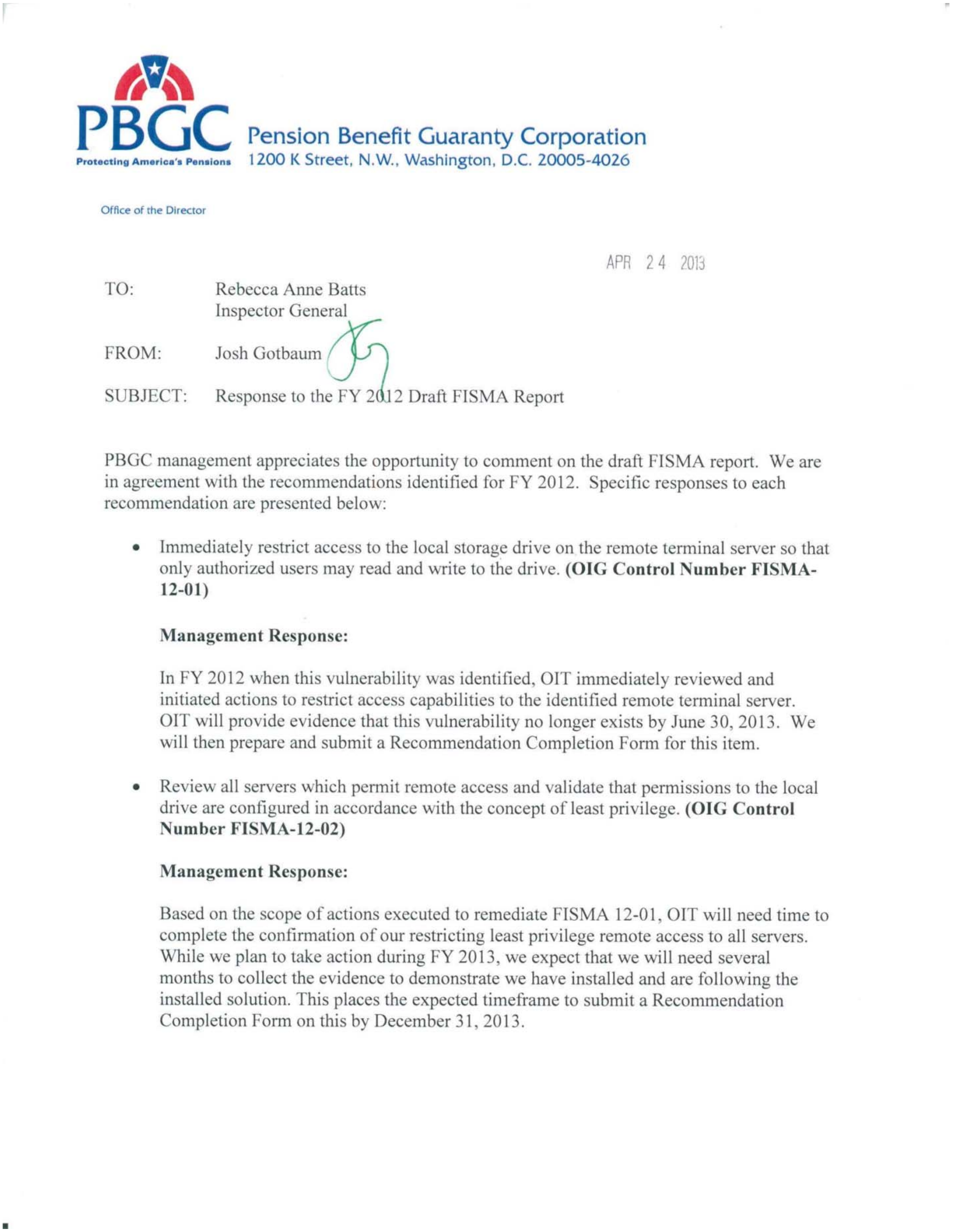
VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2011

OIG Control Number	Date Closed	Original Report Number
FISMA-11-06	October 22, 2012	EVAL-2012-9/FA-11-82-7

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-11-01	EVAL-2012-9/FA-11-82-7
FISMA-11-02	EVAL-2012-9/FA-11-82-7
FISMA-11-03	EVAL-2012-9/FA-11-82-7
FISMA-11-04	EVAL-2012-9/FA-11-82-7
FISMA-11-05	EVAL-2012-9/FA-11-82-7
Current Year	
FISMA-12-01	
FISMA-12-02	

X. MANAGEMENT RESPONSE



PBGC
Protecting America's Pensions
Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

Office of the Director

APR 24 2013

TO: Rebecca Anne Batts
Inspector General

FROM: Josh Gotbaum

SUBJECT: Response to the FY 2012 Draft FISMA Report

PBGC management appreciates the opportunity to comment on the draft FISMA report. We are in agreement with the recommendations identified for FY 2012. Specific responses to each recommendation are presented below:

- Immediately restrict access to the local storage drive on the remote terminal server so that only authorized users may read and write to the drive. **(OIG Control Number FISMA-12-01)**

  Management Response:

  In FY 2012 when this vulnerability was identified, OIT immediately reviewed and initiated actions to restrict access capabilities to the identified remote terminal server. OIT will provide evidence that this vulnerability no longer exists by June 30, 2013. We will then prepare and submit a Recommendation Completion Form for this item.

- Review all servers which permit remote access and validate that permissions to the local drive are configured in accordance with the concept of least privilege. **(OIG Control Number FISMA-12-02)**

  Management Response:

  Based on the scope of actions executed to remediate FISMA 12-01, OIT will need time to complete the confirmation of our restricting least privilege remote access to all servers. While we plan to take action during FY 2013, we expect that we will need several months to collect the evidence to demonstrate we have installed and are following the installed solution. This places the expected timeframe to submit a Recommendation Completion Form on this by December 31, 2013.

Your report also included references to prior year recommendations as well as estimated completion dates for those recommendations. In some cases, estimated completion dates have been surpassed. We are currently reviewing estimated completion dates relating to information technology issues. CCRD will coordinate with your staff after any revisions have been reviewed by the appropriate management representatives. We expect to complete this process by May 30, 2013.

Please contact Marty Boehm should you have any questions.

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