



Pension Benefit Guaranty Corporation
Office of Inspector General
Evaluation Report

**Fiscal Year 2010 Federal Information
Security Management Act (FISMA)
Independent Evaluation Report**

March 31, 2011

EVAL-2011-9/FA-10-69-8



Pension Benefit Guaranty Corporation

Office of Inspector General

1200 K Street, N.W., Washington, D.C. 20005-4026

March 31, 2011

TO: Joshua Gotbaum
Director

Richard H. Macy
Chief Information Officer

FROM: Joseph A. Marchowsky
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2010 Federal Information Security Management Act
Independent Evaluation Report (EVAL-2011-9 / FA-10-69-8)

I am pleased to transmit the fiscal year (FY) 2010 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 seventh and final report related to the FY 2010 financial statements audit.

As prescribed by FISMA, the PBGC Inspector General is required to conduct an annual evaluation of the PBGC security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this evaluation. We contracted with Clifton Gunderson LLP to complete the OMB-required responses under our direction, which we submitted to OMB on November 12, 2010. This evaluation report provides additional information on the results of Clifton Gunderson's review of the PBGC information security program.

Overall, the auditors determined that PBGC has not established an effective information security program. However, PBGC has developed and is implementing a multi-year corrective action plan (CAP) to address 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 will need to implement interim corrective actions to ensure fundamental security weaknesses do not worsen as the CAP is being implemented. The attached report contains 5 FISMA findings with 7 recommendations that are in addition to the 19 FISMA-related findings with 42 recommendations we reported in the Corporation's FY 2010 internal control report (AUD-2011-3/FA-10-69-2).

PBGC's management stated their general agreement with all recommendations. However, PBGC revised its FY 2009 approach regarding the establishment and monitoring of the entity-wide plan of action and milestones (POA&M). Before we can agree to the revised approach, OIG will need additional details to ensure that process includes the identification, review and correction of issues and items that fall outside the POA&Ms for major applications or PBGC's general support systems.

We would like to take this opportunity to express our appreciation for the overall cooperation that Clifton Gunderson and the OIG received while performing the review.

Attachment

Cc: Vince Snowbarger
Laricke Blanchard
Ann Orr
Patricia Kelly
Michael Rae
Judith Starr
Marty Boehm



March 31, 2011

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) 2010 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-10-15, *FY 2010 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.

Clifton Gunderson LLP completed the required responses on behalf of the PBGC OIG. The OIG then reviewed, approved, and submitted the responses to OMB on November 12, 2010. This evaluation report provides additional information on the results of our review of the PBGC information security program.

In preparing required responses on behalf of the OIG, we coordinated with PBGC management and appreciate their cooperation in this effort. PBGC management has provided us with a response (dated March 30, 2011) to the draft FISMA 2010 Independent Evaluation Report.

Sincerely,

CLIFTON GUNDERSON LLP

A handwritten signature in black ink that reads "George F. Fallon". The signature is written in a cursive, flowing style.

George F. Fallon, CPA
Partner

11710 Beltsville Drive
Suite 300
Calverton, Maryland 20705
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com



TABLE OF CONTENTS

	<u>Page</u>
I. EXECUTIVE SUMMARY.....	1
II. BACKGROUND.....	1
III. OBJECTIVES	2
IV. SCOPE AND METHODOLOGY.....	2
V. SUMMARY OF CURRENT YEAR TESTING	3
VI. FINDINGS AND RECOMMENDATIONS.....	4
VII. FISMA-RELATED FINDINGS INCLUDED IN THE REPORT ON INTERNAL CONTROLS	6
VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2010.....	15
IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENTDATIONS.....	15
X. MANAGEMENT RESPONSE.....	16

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 seven (7) recommendations for FY 2010 based on the results of our Fiscal Year (FY) 2010 independent evaluation. In addition, nineteen (19) FISMA-related findings with forty-two (42) recommendations were reported in the Corporation's FY 2010 internal control report based on our FY 2010 financial statements audit work. In FY 2009, 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. In response, PBGC has developed and is implementing a multi-year corrective action plan (CAP) to address 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 will need to implement interim corrective actions to ensure fundamental security weaknesses do not worsen as the CAP is being implemented.

II. BACKGROUND

The PBGC protects the pensions of nearly 44 million workers and retirees in more than 27,500 private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), as amended, 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 OIG contracted with CG to conduct PBGC's FY 2010 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) *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) *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 performing internal and external security reviews of PBGC's 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)
- Trust Accounting System (TAS)
- Spectrum Pension and Lump Sum System (PLUS)
- CoolEW2
- MyPAA

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 31, 2010 to September 30, 2010 at PBGC's headquarters in Washington DC. We also performed a security assessment of the PLUS application in July 2010 at State Street Corporation in Quincy, Massachusetts.

This independent evaluation was prepared based on information available as of September 30, 2010.

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.

PBGC's systemic security control weaknesses and the lack of an integrated financial management system continued to pose an increasing and substantial risk to PBGC's ability to carry out its mission during FY 2010. PBGC's key decision makers are acutely aware of the challenges facing the Corporation in addressing fundamental weaknesses in its IT infrastructure and environment. Management has therefore taken a multiyear approach to correct these deficiencies at the root cause level. However, in past years, communication between PBGC's key decision makers did not convey the urgent need for decisive strategic decisions to correct fundamental weaknesses in PBGC's IT infrastructure and environment. Strategic IT decisions did not address these deficiencies, and significant weaknesses identified in prior years continued to persist.

PBGC's 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 has now embarked on a more coherent strategy and cost effective approach to resolving and correcting these fundamental IT weaknesses. PBGC has developed and is implementing a multi-year corrective action plan (CAP) to address security issues at the root cause level. However, PBGC management realizes these weaknesses will continue to pose a threat to its environment for several years while corrective actions are being implemented. PBGC will need to implement interim corrective actions to ensure

fundamental security weaknesses do not worsen as the CAP is being implemented.

PBGC has entered into an interagency agreement with the Bureau of Public Debt (BPD) of the Department of the Treasury to assist PBGC in revising and strengthening its security management program and certification and accreditation (C&A) process. The multi-year CAP includes the implementation of a more effective C&A process, addressing fundamental security weaknesses and initiating an IT infrastructure modernization program. In FY 2010, PBGC procured and implemented new hardware in its infrastructure, as it works towards modernization of its IT infrastructure. Additional future actions include completing PBGC's Enterprise Architecture segment.

Our current year audit work 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 C&As of major applications and general support 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 first needs to develop and implement a framework to improve their security posture. 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 2010:

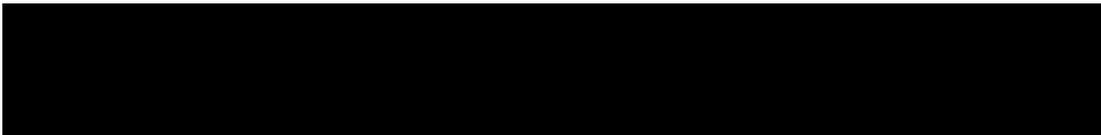
1. Entity-wide security program planning and management,
2. Access controls and configuration management,
3. Information Technology Controls for The Protection of Privacy,
4. Plan of Action and Milestones (POA&M),
5. Miscellaneous FISMA Controls.

The findings noted under 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 2009 Financial Statements Audit* (AUD-2011-2/FA-10-69-1) issued on November 12, 2010. 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-10-15 which are included in this report. These findings and recommendations, not previously reported, are as follows.

VI. FINDINGS AND RECOMMENDATIONS

1. Access controls and configuration management

- 

[REDACTED]

Recommendation:

Expedite the implementation of an accepted or validated cryptographic module [REDACTED]

[REDACTED]

Control Number # FISMA-10-01) NFR #29

(OIG

2. Privacy

- Technical controls related to the protection of Personally Identifiable Information (PII) need to be strengthened. Based on our FY 2009 and FY 2010 reviews, we noted that:
 - No encryption mechanism was in place on PBGC laptops.

Any unauthorized use, disclosure, or loss of PII data can result in the loss of the public's trust and confidence in PBGC's ability to properly protect it. PII data breaches may have far-reaching implications for individuals whose PII is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. A PII data breach may also require significant PBGC staff, time, assets, and financial resources to mitigate the negative consequences, which may prevent PBGC from allocating those resources elsewhere.

Recommendation:

Implement encryption on all PBGC's laptops to ensure that PII is adequately protected. **(OIG Control Number FISMA-09-07) NFR #38**

3. POA&M

- PBGC management did not provide CG with a copy of the entity-wide POA&M. Lack of an up-to-date and consolidated POA&M could result in security deficiencies identified not being properly tracked and monitored, and thereby not remediated in a timely manner.

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) NFR #39**

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

Recommendations:

- Ensure that the agency and program specific POA&M is tracked appropriately and is provided to PBGC's CIO regularly. **(OIG Control Number FISMA-09-10) NFR #20**
- 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) NFR #20**

4. Miscellaneous FISMA Controls

- PBGC has not included information about its IT security policies and requirements including use of NIST common security configurations in all of its IT contracts as required by FAR § 39.101(d).

Recommendation:

Ensure all PBGC IT acquisitions include appropriate language as required by FAR § 39.101(d). **(OIG Control Number FISMA-09-12) NFR #40**

VII. FISMA-Related Findings Included in the Report on Internal Controls

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 2010 and 2009 Financial Statements Audit* (AUD-2011-2/FA-09-69-1) issued November 12, 2010.

Finding Summary	Recommendation
<p>1. PBGC identified 65 common security controls for the 17 National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, security control families. Of the 65 common security controls tested by PBGC in FY 2008, only four controls were properly designed and operating effectively. PBGC did not continue its implementation of common controls in FY 2009 and FY 2010. 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. Consequently, PBGC has not completed and confirmed the design, implementation, and operating effectiveness of its common security controls. Without testing control processes, management cannot have confidence that the controls were implemented.</p>	<p>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)</p> <p>Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. (OIG Control # FS-08-01)</p> <p>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)</p>
<p>2. PBGC's process for the completion of C&A packages in accordance with NIST SP 800-37, <i>Guide for the Security Certification and Accreditation of Federal Information Systems</i>, is ineffective. Fundamental weaknesses in PBGC's infrastructure architecture and design do not support the C&A of its information systems. Furthermore, PBGC's information systems employ obsolete and antiquated technologies that pose</p>	<p>Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies. (OIG Control # FS-09-03)</p> <p>Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of</p>

Finding Summary	Recommendation
<p>additional risk to the availability of financially significant systems. PBGC abandoned its C&A packages and is working with BPD to revise and strengthen its C&A process to ensure security weaknesses are addressed at the root cause level. PBGC did not conduct C&As in FY 2010. The Corporation has implemented a multi-year plan to correct its C&As.</p>	<p>technologies to support a more coherent approach to providing information services and information system management controls. (OIG Control # FS-09-04)</p> <p>Implement an effective review process to validate the completion of the C&A packages for all major applications and general support systems. The review should not be performed by an individual associated with the performance of the C&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)</p> <p>Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the C&A process. (OIG Control # FS-09-05)</p> <p>Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the certification and review process. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. (OIG Control # FS-09-06)</p> <p>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 # FS-09-07)</p> <p>Implement an independent and effective review process to validate the completion of the C&A packages for all applications and 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)</p>

Finding Summary	Recommendation
	<p>Implement robust and rigorous review procedures to verify that future contracts for the C&A of PBGC's systems clearly outline expectations and deliverables in the statement of work. (OIG Control # FS-09-08)</p> <p>Implement a robust and rigorous quality review process to verify contractor C&A deliverables meet the requirements specified in the statement of work. (OIG Control # FS-09-09)</p> <p>Establish controls to ensure that contract staff tasked with the C&A of PBGC systems have the appropriate knowledge and background to accurately and comprehensively complete the C&A process. (OIG Control # FS-09-10)</p> <p>Implement a robust and rigorous process to verify compliance with PBGC's policy on contractor management throughout the C&A lifecycle. (OIG Control # FS-09-11)</p>
<p>3. Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for Security Awareness training.</p>	<p>Develop and implement a process to enforce the dissemination and awareness of PBGC's security policies and procedures through adequate training. (OIG Control # FS-07-04)</p>
<p>4. OIT and system owners (i.e. business owners) have not established and documented service level agreements that include metrics on OIT services required to meet business goals. PBGC is in the process of completing the development and distribution of measurable services provided to the business owners by the OIT.</p>	<p>Establish, document, and publish measurable services that OIT provides to the Corporation, that are acceptable to all information system owners. (OIG Control # FS-07-06)</p>
<p>5. PBGC's benefit payments service provider (service provider) implemented a security operations center outside of the United States, which will have some responsibility for monitoring security related events associated with the Pension Lump Sum (PLUS) application and components of its system boundary.</p>	<p>Develop and implement an immediate plan of action to address the potential security risk posed by locating the Security Operations Center outside of the US. (OIG Control # FS-10-01)</p> <p>Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and FISMA. (OIG Control #</p>

Finding Summary	Recommendation
<p>The service provider did not provide PBGC with adequate advance notice to assess the security impact to the PLUS application on the change in environment before going operational. Furthermore, PBGC was not provided adequate time to assess risks to its systems and implement mitigating controls to ensure compliance with the PBGC's policies and procedures. As a result, PBGC has not assessed the security impact of the change in environment.</p>	<p>FS-10-02)</p>
<p>6. PBGC has not executed an interconnection security agreement (ISA) or memorandum of understanding (MOU) between external organizations whose systems interconnect with PBGC's systems.</p> <p>PBGC is in the process of planning and documenting security agreements for interconnection with 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 details that may be required to provide overall security for systems that are interconnected.</p>	<p>Develop and implement an ISA and MOU with external organizations whose systems connect to PBGC's systems. (OIG Control # FS-10-03)</p>
<p>7. 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.</p>	<p>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)</p> <p>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)</p>

Finding Summary	Recommendation
	<p>Establish baseline configuration standards for all of PBGC's systems. (OIG Control # FS-09-13)</p> <p>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)</p> <p>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)</p> <p>Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. (OIG Control # FS-09-16)</p>
<p>8. 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.</p>	<p>Continue to remove unnecessary user and/or generic accounts. (OIG Control # FS-07-08)</p>
<p>9. 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.</p>	<p>Consistently implement controls to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. (OIG Control # FS-07-09)</p> <p>Assess the risk associated with lacking 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</p>

Finding Summary	Recommendation
	acceptance. (OIG Control # FS-09-17)
<p>10. 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.</p>	<p>Appropriately restrict developers' access to production environment to only temporary emergency access. (OIG Control # FS-07-10)</p> <p>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 # FS-09-18)</p>
<p>11. Controls are not consistently applied to ensure that authentication parameters for general support systems (e.g. Novell, Windows, SUN Solaris, Oracle, etc.) and applications are in compliance with the 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.</p>	<p>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 Information Assurance Handbook (IAH). (OIG Control # FS-07-11)</p> <p>Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. (OIG Control # FS-09-19)</p>
<p>12. PBGC is still in the process of identifying dependencies between databases, applications, and operating systems in order to fully implement controls to lock out and remove inactive and dormant accounts. However, there are still some PBGC systems that have not implemented these controls.</p>	<p>For the remaining systems, apply controls to lock out and remove inactive and dormant accounts after a specified period in accordance with the IAH. (OIG Control # FS-07-12)</p>
<p>13. 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 1.2, does not explicitly state that all accounts (e.g. user, system, and service) across all platforms and</p>	<p>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)</p>

Finding Summary	Recommendation
applications will be re-certified annually.	
<p>14. 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.</p>	<p>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)</p> <p>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)</p>
<p>15. 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.</p>	<p>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 # FS-07-15)</p>
<p>16. PBGC lacks an effective process to track contractors throughout their employment at PBGC, including appropriate notifications of start dates and separation. Management has reported that policies and procedures, to include PBGC Directive PM 05-1, <i>PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees</i> have not been updated to provide effective enforcement of controls designed to track entrance and separation of all Federal and contract employees.</p>	<p>Update and enforce directive PM 05-1, <i>PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees</i>, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. (OIG Control # FS-07-16)</p>
<p>17. Periodic logging and monitoring of security-related events for PBGC's applications were inadequate for CFS, PAS, TAS, Participant Records Information Systems Management (PRISM), and Integrated Present Value of Future Benefits (IPVFB) System. PBGC's information technology infrastructure consist of multiple legacy systems and applications (e.g. PAS, TAS, IPVFB, PRISM, GENESIS database, Solaris 8,</p>	<p>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)</p>

Finding Summary	Recommendation
<p>Oracle 8i, Novell NetWare 5.1, Windows NT, etc.) that do not have a coherent architecture for management and security.</p>	
<p>18. 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 C&A of the PLUS application. Although continuous monitoring was implemented, no alerts were provided to PBGC about the application virtualization/application becoming obsolete and the potential security risk to PLUS. Obsolete software may expose PBGC's infrastructure to a security-related vulnerability. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected.</p>	<p>Replace the Citrix MetaFrame presentation server. (OIG Control # FS-10-04)</p> <p>Include the application virtualization/application delivery product used by the benefits payments service provider to access the PLUS application in the system boundary. (OIG Control # FS-10-05)</p>
<p>19. The TeamConnect application, which replaced the Lotus Notes system in FY 2010, maintains a nightly premium output batch file error log in a .txt file format, which can be edited. Management has not locked down the TeamConnect output file from manipulation. Because the exception log data can be manipulated, the Actuarial database into which the data is being transferred may be compromised or corrupted. Unresolved inaccuracies between the Corporate Data Management System and the Actuarial Database could result in errors in the amount of contingent liabilities recorded and disclosed in the financial statement.</p>	<p>Configure TeamConnect to ensure the integrity of the nightly premium output batch file error log. (OIG Control # FS-10-06)</p>

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2010

<u>OIG Control Number</u>	<u>Date Closed</u>	<u>Original Report Number</u>
FISMA-09-01	9/22/10	AUD-2010-6/FA-09-64-6
FISMA-09-02	9/22/10	AUD-2010-6/FA-09-64-6
FISMA-09-03	9/22/10	AUD-2010-6/FA-09-64-6
FISMA-09-04	9/22/10	AUD-2010-6/FA-09-64-6
FISMA-09-05	9/22/10	AUD-2010-6/FA-09-64-6
FISMA-09-06	9/22/10	AUD-2010-6/FA-09-64-6

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

<u>OIG Control Number</u>	<u>Original Report Number</u>
<i>Prior Year</i>	
FISMA-09-07	AUD-2010-6/FA-09-64-6
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-09-12	AUD-2010-6/FA-09-64-6
<i>Current Year</i>	
FISMA-10-01	

X. Management Response



To: Rebecca A. Batts
Inspector General

From: Richard Macy 
Chief Information Officer

Subject: Management Response to the Draft FISMA Report for FY 2010

Date: March 30, 2011

On behalf of PBGC management, I write to provide our comments on the draft report. We appreciate the opportunity to comment and your continued support in identifying ways to improve our internal controls, especially those relating to IT security.

We are in general agreement with the recommendations contained in the report. In the Attachment 1 to this memorandum, we have provided our specific responses to the recommendations contained in the draft report.

Please contact Marty Boehm should you have any questions regarding this response.

Attachment

Management Response to the Draft FISMA Report for FY 2010

OIG Recommendation No. OIT/FISMA-10-01: Expedite the implementation of an accepted or validated cryptographic module [REDACTED]

Management Response:

We agree. [REDACTED]

OIG Recommendation No. OIT/FISMA-09-07: Implement encryption on all PBGC's laptops to ensure that PII is adequately protected.

Management Response:

We agree and will submit for your consideration evidence that we completed this recommendation in December 2010 for all PBGC laptops, with two exceptions.

OIG Recommendation No. OIT/FISMA-09-08: 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 Recommendation No. OIT/FISMA-09-09: Disseminate PBGC's entity wide POA&M to all responsible parties to ensure corrective actions are taken in accordance with POA&M.

OIG Recommendation No. OIT/ FISMA-09-10: Ensure that the agency and program specific POA&M is tracked appropriately and is provided to PBGC's CIO regularly.

OIG Recommendation No. OIT/FISMA-09-11: Ensure PBGC's CIO centrally tracks, maintains and independently reviews/validates POA&M activities, at least on a quarterly basis.

Management Response to FISMA-09-08, 09-09, 09-10 & 09-11: We agree with the findings and would like to suggest an alternative to the specific recommendations offered. PBGC is developing an agency wide POA&M program and process to be managed by the Senior Agency Information Security Officer that will ensure system POA&Ms are identified, tracked, analyzed, solved and reported on with consistency and discipline. The analysis will include identification of POA&Ms with similarities across systems as well as consistency of solutions. The program will provide reporting on POA&M status and progress at least quarterly to the CIO and when

Management Response to the Draft FISMA Report for FY 2010

warranted to the EMC to ensure POA&Ms are completed as planned as well as to provide visibility to the IT-specific control and security risks to the agency. For common control POA&Ms that apply to PBGC as a whole, we plan to track those items in one of the two General Support System (GSS) POA&Ms. We expect to establish the POA&M program by the end of FY11 and have the two GSS system POA&Ms managed according to the new program. Other applications will come under the new POA&M program during FY11 and FY12 either through a new Assessment and Authorization effort for the application or by converting existing application-specific POA&Ms into the new program.

OIG Recommendation No. PD/FISMA-09-12: Ensure all PBGC IT acquisition include appropriate language as required by FAR Part 39 101 (d).

Management Response: We agree. PBGC has developed contract language for new externally hosted/run systems to ensure vendors know their security and control responsibilities under FISMA. Additionally, PBGC will prepare a package to demonstrate that existing vendors have the appropriate language as required by FAR Part 39 101 (d).

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