



Pension Benefit Guaranty Corporation
Office of Inspector General
Evaluation Report

**Fiscal Year 2009 Federal Information
Security Management Act (FISMA)
Independent Evaluation Report**

March 22, 2010

EVAL-2010-7 / FA-09-64-7



Pension Benefit Guaranty Corporation

Office of Inspector General

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

March 22, 2010

To: Richard H. Macy
Chief Operating Officer and Acting Chief Information Officer

From: *for* Joseph A. Marchowsky *Joseph A. Marchowsky*
Assistant Inspector General for Audit

Subject: Fiscal Year 2009 Federal Information Security Management Act
Independent Evaluation Report (EVAL-2010-7 / FA-09-64-7)

I am pleased to transmit the fiscal year (FY) 2009 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 fiscal year 2009 financial statements audit (AUD-2010-1/FA-09-64-1).

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. Clifton Gunderson LLP, on behalf of the PBGC OIG, completed the OMB-required responses that we then submitted to OMB on November 18, 2009. 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 and has not been proactive in reviewing security controls and identifying areas to strengthen this program. The attached report contains 6 FISMA findings with 12 recommendations. In addition, 15 FISMA-related findings with 36 recommendations were reported in the Corporation's FY 2009 internal control report (AUD-2010-2/FA-09-64-2).

The response to a draft of this report indicates PBGC management's general agreement with all recommendations and provided specific responses for each recommendation. Further, PBGC management is currently preparing their initial corrective action plan to address the material weakness reported in the FY 2009 financial statements audit. Where appropriate, PBGC management considers findings and recommendations relating to the FISMA report as part of that process and expects to present their initial corrective action plan in April 2010.

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

Attachment

cc: Vincent K. Snowbarger
Stephen E. Barber

Terrence M. Deneen
Patricia Kelly

Judith R. Starr
Martin O. Boehm

Fiscal Year 2009 FISMA Independent Evaluation Report

EVAL-2010-7 / FA-09-64-7

Contents

| | Page |
|--|------|
| Independent Auditor's FISMA Evaluation Report | 1 |
| Section | |
| I. Executive Summary | 2 |
| II. Background | 2 |
| III. Objectives | 3 |
| IV. Scope and Methodology | 3 |
| V. Summary of Current Year Testing | 4 |
| VI. Findings and Recommendations | 5 |
| VII. Previously Reported FISMA-Related Findings | 10 |
| VIII. FISMA Recommendations Closed in Fiscal Year 2009 | 16 |
| IX. Prior and Current Years' Open FISMA Recommendations | 16 |
| X. Management Response | 17 |

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) 2009 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-09-29, "FY 2009 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 18, 2009. 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. In its response to a draft of this report, PBGC management was in general agreement with the recommendations contained in the report and provided specific responses to each recommendation. Management's response is included in its entirety in Section X of this report.

Clifton Gunderson LLP

Calverton, Maryland
November 18, 2009

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 six (6) FISMA findings with twelve (12) recommendations for FY 2009 based on the results of our Fiscal Year (FY) 2009 independent evaluation. In addition, fifteen (15) FISMA-related findings with thirty-six (36) recommendations were reported in the Corporation's FY 2009 internal control report based on our FY 2009 financial statements audit work. Overall, we determined that the Pension Benefit Corporation (PBGC) has not established an effective information security program and has not been proactive in reviewing security controls and identifying areas to strengthen this program.

II. BACKGROUND

The Pension Benefit Guaranty Corporation (PBGC) protects the pensions of nearly 44 million workers and retirees in more than 29,000 private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on information technology (IT). Internal controls over these operations are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

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

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

PBGC operates an open and distributed computing environment to facilitate collaboration and knowledge sharing, and support its mission of protecting the pensions of nearly 44 million workers and retirees. It faces the challenging task of maintaining this environment, while protecting its critical information assets against malicious use and intrusion.

The PBGC Office of Inspector General (OIG) contracted with Clifton Gunderson LLP (CG) to conduct PBGC's FY 2009 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 AND METHODOLOGY

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

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

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

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

- Consolidated Financial System (CFS)
- Premium Accounting System (PAS)
- Integrated Present Value of Future Benefits (IPVFB)
- Pension and Lump Sum System (PLUS)
- ComprizonSuite
- Administar

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 March 24, 2009 to September 30, 2009 at PBGC's headquarters in Washington DC. We also performed a security assessment of the PLUS application in July 2009 at State Street Corporation in Quincy, Massachusetts. This independent evaluation was prepared based on information available as of September 30, 2009.

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 posed increasing and substantial risk to PBGC's ability to carry out its mission during FY 2009. 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. Furthermore, these weaknesses were not addressed in the status of corrective actions being reported. As a result, PBGC's attempt to address entity-wide security management program deficiencies and systemic security control weaknesses at the root cause level had minimal effect.

PBGC's 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.

PBGC's management is starting to take actions to correct control weaknesses by conducting an assessment of its Oracle database environment, initiating an IT Infrastructure modernization program, completing the Enterprise Architecture (EA) segment architecture, and implementing strategic decisions on IT sourcing.

Our current year audit work found 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 certification and accreditation 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 that significant deficiencies in the following areas constitute a material weakness for FY 2009:

1. Entity-wide security program planning and management,

2. Access controls and configuration management,
3. 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 2009 and 2008 Financial Statements Audit* (AUD-2010-2/FA-09-64-2) issued on November 12, 2009. 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-09-29 which are included in this report. These findings and recommendations, not previously reported, are as follows.

VI. FINDINGS AND RECOMMENDATIONS

1. Privacy

- The PBGC's Privacy Office does not properly monitor its privacy processes for quality and compliance. We noted the following weaknesses:
 - Privacy Impact Assessments (PIAs) for PBGC's major applications and general support systems were not updated on an annual basis in accordance with PBGC Information Assurance Handbook, Volume 12.
 - The PIA Executive Summary for the major applications posted on PBGC's Internet was updated in March 2007 and does not reflect current PIAs conducted.
 - System of Records Notices (SORNs) for nine (9) out of fourteen (14) PBGC's major applications and general support systems are not current as there were subsequent changes to the system after which a SORN was not updated.

PBGC's Information Assurance Handbook (IAH), Volume 12 Security Planning Procedures requires the Information System Security Officer (ISSO) and Information System Owners to complete the PIA before collecting information in an identifiable form. The PIA is then reviewed and approved by PBGC's Privacy Officer.

PBGC contracted for assessment of its Oracle database in 2009 and issued an Oracle Assessment Report in March 2009. The report identified several weaknesses related to protecting personally identifiable information (PII), including the following:

- PII existed in the development environment.
- PBGC does not encrypt its backup tapes, putting PII data at risk when it leaves the datacenter.

- There is nothing in the PBGC IT environment (i.e. production, test, and development environments) that prevents the loss of PII data. If somebody were to get access to the backup data, they would have unfiltered access to all data elements including PII.

Recommendations:

- Review and update the Privacy Impact Assessments (PIAs) at least annually in accordance with PBGC's Information Assurance Handbook. **(OIG Control Number FISMA-09-01)**

Management's Response: PBBC agreed.

- Conduct an annual review of the PIAs on the PBGC's website to verify that it reflects the most updated PIAs conducted. **(OIG Control Number FISMA-09-02)**

Management's Response: PBBC agreed.

- Review and update the System of Records Notice (SORNs) periodically, at least annually, to reflect current conditions. **(OIG Control Number FISMA-09-03)**

Management's Response:

PBGC agreed in part and is assigning additional legal staff from the Office of General Counsel to review and update existing Privacy Act System of Records Notices (SORNs) for publication in the Federal Register. On January 8, 2010, the Privacy Officer sent a copy of the existing SORNs to the designated manager of each system of records for review, and requested the submission of any proposed changes to the SORN from the manager. As of March 10, 2010, all system owners had responded. PBGC expects to complete this aspect of the recommendation by June 1, 2010.

In addition, the Privacy Officer will establish procedures to send a notice by May 1st of every other year to the designated manager of each existing Privacy Act System of Records that requests the manager to certify that the SORN remains accurate and up-to-date, and if not, to submit proposed changes to the Privacy Officer within 30 days. Under Appendix 1 to OMB Circular No. A-130, Management of Federal Information Resources, dated November 28, 2000; PBGC is required to review SORNs at least once every two years, not annually. PBGC expects to complete this aspect of the recommendation by September 30, 2010.

CG's Evaluation of Management's Response:

We believe the actions proposed by PBGC management are responsive to our recommendation.

- PBGC's process for reporting PII incidents is inaccurate and unverifiable. We could not verify or validate log entries on incidents reported to the United States Computer Emergency Readiness Team (US-CERT). Evidence provided could not be traced to incidents reported to US-CERT.

We also noted inconsistencies in the reporting of similar PII breaches to US-CERT. Our review of PBGC's FY 2009 PII incident log noted that only six (6) of nineteen (19) PII incidents were reported to US CERT. For example, similar PII incidents such as an incident dated 10/24/08, disclosing a participant's social security number (SSN), was not reported to US CERT, however, an incident on 11/12/08, disclosing a participant's SSN, was reported to US-CERT. Furthermore, PBGC does not have reporting guidelines for reporting PII incidents.

Without timely and effective remediation of PII incidents, PBGC is at risk for similar compromises which may result in participant personal information being at risk.

Recommendations:

- Develop and follow specific guidance on how and when to report incidents, involving PII disclosure. **(OIG Control Number FISMA-09-04)**

Management's Response: PBGC agreed.

- Ensure all incidents involving PII are reported to US CERT within 1 hour of discovery. **(OIG Control Number FISMA-09-05)**

Management's Response: PBGC agreed.

- Ensure all reports submitted to US-CERT are documented and maintained appropriately. **(OIG Control Number FISMA-09-06)**

Management's Response: PBGC agreed.

- Technical controls related to the protection of PII need to be strengthened. Based on our review, we noted that:
 - No encryption mechanism was in place on PBGC laptops.
 - No formalized procedures were in place to control laptops leaving PBGC premises

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)**

Management's Response: PBBC agreed.

2. Plan of Action and Milestones (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 will 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)**

Management's Response: PBBC agreed.

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

Management's Response: PBBC agreed.

- PBGC's POA&M process is ineffective. We noted the following deficiencies in FY 2009:
 - 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, maintaining and independently reviews/validates POA&M activities on at least a quarterly basis.

Recommendations:

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

Management's Response: PBBC agreed.

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

Management's Response: PBBC agreed.

3. 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 acquisition include appropriate language as required by FAR § 39.101(d). **(OIG Control Number FISMA-09-12)**

Management's Response: PBBC agreed.

VII. PREVIOUSLY REPORTED FISMA-RELATED FINDINGS

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 2009 and 2008 Financial Statements Audit* (AUD-2010-2/FA-09-64-2) issued November 12, 2009.

| Finding Summary | Recommendation |
|---|---|
| <p>1. PBGC has identified sixty-five (65) common security controls for the seventeen (17) NIST SP 800-53, <i>Recommended Security Controls for Federal Information Systems</i>, security control families. Of the 65 common security controls tested by PBGC, only four controls were properly designed and operating effectively. Weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications have adversely affected its ability to effectively implement common security controls across its systems and applications.</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 Number FS-09-01)</p> <p>Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. (OIG Control Number 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 Number 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 certification and accreditation of its information systems. Furthermore, PBGC's information systems employ obsolete and antiquated technologies that pose additional risk to the availability of financially significant systems.</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 Number FS-09-03)</p> <p>Complete the development and implementation of the redesign of PBGC's IT infrastructure and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. (OIG Control Number FS-09-04)</p> <p>Implement an effective review process to validate the completion of the certification and accreditation packages for all major</p> |

| Finding Summary | Recommendation |
|-----------------|---|
| | <p>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 Number 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 Number 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 Number 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 OIT operations. (OIG Control Number FS-09-07)</p> <p>Implement an independent and effective review process to validate the completion of the certification and accreditation 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 Number FS-08-03)</p> <p>Implement robust and rigorous review procedures to verify that future contracts for the Certification and Accreditation of PBGC's systems clearly outline expectations and deliverables in the statement of work. (OIG Control Number FS-09-08)</p> <p>Implement a robust and rigorous quality review process to verify contractor C&A</p> |

| Finding Summary | Recommendation |
|---|--|
| | <p>deliverables meet the requirements specified in the statement of work. (OIG Control Number 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 Number 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 Number 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 Number FS-07-04)</p> |
| <p>4. Office of Information Technology (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.</p> | <p>Establish, document, and publish measurable services that OIT provides to the Corporation, that are acceptable to all information system owners. (OIG Control Number FS-07-06)</p> |
| <p>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 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 Number 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 Number FS-09-12)</p> <p>Establish baseline configuration standards for all of PBGC's systems. (OIG Control Number</p> |

| Finding Summary | Recommendation |
|--|---|
| | <p>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 Number FS-09-14)</p> <p>Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance. (OIG Control Number FS-09-15)</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 Number FS-09-16)</p> |
| <p>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. 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 Number FS-07-08)</p> |
| <p>7. 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 Number 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 acceptance. (OIG Control Number FS-09-17)</p> |

| Finding Summary | Recommendation |
|---|--|
| <p>8. 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 Number 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 Number FS-09-18)</p> |
| <p>9. 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 IAH. (OIG Control Number FS-07-11)</p> <p>Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. (OIG Control Number FS-09-19)</p> |
| <p>10. 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 Number FS-07-12)</p> |
| <p>11. 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 applications will be re-certified annually.</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 Number FS-07-13)</p> |

| Finding Summary | Recommendation |
|---|--|
| <p>12. 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 Number 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 Number FS-09-20)</p> |
| <p>13. 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 Number FS-07-15)</p> |
| <p>14. 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, PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees 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 Number FS-07-16)</p> |
| <p>15. Periodic logging and monitoring of security-related events for PBGC's applications were inadequate CFS, PAS, Trust Accounting System (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, Oracle 8i, Novell NetWare 5.1, Windows NT, etc.) that do not have a coherent architecture for the management and security of these systems.</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 Number FS-07-17)</p> |

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2009

| <u>OIG Control Number</u> | <u>Date Closed</u> | <u>Original Report Number</u> |
|---------------------------|--------------------|-------------------------------|
| None | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

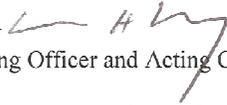
IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

| <u>OIG Control Number</u> | <u>Original Report Number</u> |
|----------------------------|-------------------------------|
| | |
| <u>Prior Year</u> | |
| None | |
| | |
| | |
| | |
| | |
| | |
| | |
| <u>Current Year</u> | |
| FISMA-09-01 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-02 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-03 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-04 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-05 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-06 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-07 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-08 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-09 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-10 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-11 | EVAL-2010-7/FA-09-64-7 |
| FISMA-09-12 | EVAL-2010-7/FA-09-64-7 |
| | |
| | |
| | |
| | |
| | |
| | |

X. MANAGEMENT RESPONSE



To: Rebecca A. Batts
Inspector General

From: Richard Macy 
Chief Operating Officer and Acting Chief Information Officer

Subject: Management Response to the Draft FISMA Report for FY 2009

Date: March 10, 2010

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 Attachment A to this memorandum, we have provided our specific responses to the recommendations contained in the draft report. As we have informed your office, we are currently preparing our initial corrective action plan to address the material weakness reported by Clifton Gunderson LLP as part of the FY 2009 financial statement audit. We are considering findings and recommendations relating to this report as part of that process, where appropriate. We expect to present our initial corrective action plan in April of this year.

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

Attachment

Management Response to the Draft FISMA Report for FY 2009

OIG Recommendation No. OGC/FISMA-09-01: Review and update the Privacy Impact Assessments (PIAs) at least annually in accordance with PBGC's Information Assurance Handbook.

Management Response: We agree. On January 7, 2010, PBGC's Privacy Officer sent a notice to PBGC Information System Owners requesting them to certify that the PIA for their systems remain accurate and up-to-date, and if not, to submit proposed changes by February 8, 2010, for review and incorporation into a revised PIA. Because the Federal government was closed due to inclement weather, the Privacy Officer extended the deadline for information system owners to respond to February 24, 2010. Please note that the Privacy Officer and his staff are following up with the owner of one system who has been out of the office and has not yet responded.

In addition, the Privacy Officer will establish procedures to send a notice to PBGC Information System Owners by May 1 of each subsequent year requesting them to certify that their PIAs remain accurate and up-to-date, and if not, to submit proposed changes within 30 days for review and incorporation into a revised PIA. We expect to complete work on this recommendation by September 30, 2010.

OIG Recommendation No. OGC/FISMA-09-02: Conduct an annual review of the PIAs on the PBGC's website to verify that it reflects the most updated PIAs conducted.

Management Response: We agree. PBGC's Privacy Officer will review the responses to the request for certification of PIAs discussed above, and make any necessary changes to the Executive Summary of the PIA that is posted publicly on PBGC's website. We expect to complete work on this recommendation by June 30, 2010.

OIG Recommendation No. OGC/FISMA-09-03: Review and update the System of Records Notice (SORNs) periodically, at least annually, to reflect current conditions.

Management Response: We agree in part. OGC is assigning additional legal staff to review and update existing Privacy Act System of Records Notices (SORNs) for publication in the Federal Register. On January 8, 2010, the Privacy Officer sent a copy of the existing SORNs to the designated manager of each system of records for review, and requested the submission of any proposed changes to the SORN from the manager. All system owners have now responded. We expect to complete this aspect of the recommendation by June 1, 2010.

In addition, the Privacy Officer will establish procedures to send a notice by May 1st of every other year to the designated manager of each existing Privacy Act System of Records that requests the manager to certify that the SORN remains accurate and up-to-date, and if not, to submit proposed changes to the Privacy Officer within 30 days. Please note, however, that under Appendix 1 to OMB Circular No. A-130, Management of Federal Information Resources, (Nov.

Management Response to Draft FISMA Report for FY 2009

28, 2000), PBGC is required to review SORNs at least once every two years, not annually. We expect to complete this aspect of the recommendation by September 30, 2010.

OIG Recommendation No. OGC/FISMA-09-04: Develop and follow specific guidance on how and when to report incidents, involving PII disclosure.

Management Response: We agree. With input from the Acting Chief Information Officer (CIO) and Acting Senior Agency Information Security Officer (SAISO), OGC has established specific guidance and procedures for OGC's privacy staff to follow to report security incidents involving PII disclosure to US-Cert. PBGC's Information Systems Security Officer (ISSO) has been directed to notify OGC's privacy staff of all security incidents involving PII that are reported under the policies and procedures outlined in Volume 8 of PBGC's Information Assurance Handbook. We have completed action on this recommendation and will be forwarding supporting documentation to the OIG shortly.

OIG Recommendation No. OGC/FISMA -09-05: Ensure all incidents involving PII are reported to US CERT within 1 hour of discovery.

Management Response: We agree. As part of specific guidance and procedures to be developed by January 30, 2010, OGC has implemented a two-step US-Cert reporting process. Within one hour of when an incident is reported to OGC, OGC will make a preliminary report to US Cert using its on-line reporting system. In response, US-Cert will e-mail PBGC an incident report number. OGC will then investigate the incident to confirm the relevant facts and send any necessary follow-up report to US-Cert. According to US-Cert, an agency can update an incident report by sending an e-mail to US-Cert that includes the incident report number in the subject line. We have completed action on this recommendation and will be forwarding supporting documentation to the OIG shortly.

OIG Recommendation No. OGC/FISMA -09-06: Ensure all reports submitted to US-CERT are documented and maintained appropriately.

Management Response: We agree. OGC has devised a record-keeping plan to ensure that preliminary and follow-up reports to US Cert are maintained. We have completed action on this recommendation and will be forwarding supporting documentation to the OIG shortly.

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. OIT is currently in the planning process for laptop encryption with a tentative scheduled project completion date of September 30, 2010.

Management Response to Draft FISMA Report for FY 2009

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.

Management Response: We agree. PBGC is working with the Bureau of Public Debt to reestablish our Security Program. Work on policy and procedure development is anticipated to be completed by September 30, 2010. A timetable for implementing the changes to the program will be developed at that time, which will include standing up an entity-wide POAM and the ongoing maintenance and reporting thereof.

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.

Management Response: We agree. PBGC is working with the Bureau of Public Debt to reestablish our Security Program. Work on policy and procedure development is anticipated to be completed by September 30, 2010. A timetable for implementing the changes to the program will be developed at that time, which will include standing up our system-specific POAMs and the ongoing maintenance and reporting thereof.

OIG Recommendation No. OIT/FISMA-09-10: Ensure that the agency and program specific plan of action and milestones are tracked appropriately and is provided to PBGC's CIO regularly.

Management Response: We agree. PBGC is working with the Bureau of Public Debt to reestablish our Security Program. Work on policy and procedure development is anticipated to be completed by September 30, 2010. A timetable for implementing the changes to the program will be developed at that time, which will include standing up our agency and system-specific POAMs and the ongoing and reporting thereof.

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: We agree. PBGC is working with the Bureau of Public Debt to reestablish our Security Program. Work on policy and procedure development is anticipated to be completed by September 30, 2010. A timetable for implementing the changes to the program will be developed at that time, which will include standing up our POAMs and the ongoing maintenance and reporting thereof.

Management Response to Draft FISMA Report for FY 2009

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. In cooperation with the Office of the General Counsel and OIT's Enterprise Information Security Office, the Procurement Department has developed a local clause which will be included in future solicitations for information technology, as required by FAR 39.101(d). The clause is presented below:

PBGC-04-006 Common Security Configurations For Information Technology Acquisition (Nov 2009): In acquiring Information Technology (IT) assets for the Government, the Contractor shall incorporate and comply with the latest version of all applicable information technology security policies and requirements, including, but not limited to, those published by PBGC, and the common security configurations defined by the National Institute of Standards and Technology [NIST] at <http://web.nvd.nist.gov/view/nep/repository> and <http://checklist.nist.gov> which are generally for desktop operating systems (Windows XP or VISTA). When incorporating such security configuration requirements in contracts, the contractor can consult the Contracting Officer's Technical Representative to determine the appropriate configuration reference for a particular system or services acquisition. The Contractor shall ensure all its subcontractors which perform work under this contract comply with the above requirements.

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