



Pension Benefit Guaranty Corporation
Office of Inspector General
Audit Report

**Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's Fiscal
Year 2009 and 2008 Financial Statements Audit**

November 12, 2009

AUD-2010-2 / FA-09-64-2



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

November 12, 2009

To: Patricia Kelly
Chief Financial Officer

From: Joseph A. Marchowsky
Assistant Inspector General for Audit

Subject: 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)

I am pleased to transmit the attached report prepared by Clifton Gunderson LLP resulting from their audit of the PBGC Fiscal Year 2009 and 2008 Financial Statements. The purpose of this report is to provide more detailed discussions of the specifics underlying the significant deficiencies and material weakness reported in the internal control section of the combined Independent Auditor's Report dated November 12, 2009 (AUD-2010-1/FA-09-64-1). The attached management response to a draft of this report indicates management's agreement with each recommendation and their commitment to addressing the recommendations contained in the report and to remediating the associated material weakness.

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

Attachment

cc: Vince Snowbarger	Robert Callahan	Pat Kieth
Stephen Barber	David Harvey	Michael Zacour
Terrence Deneen	Beverly Hebron	Ray Reigle
Richard Macy	Lashon Lissimore	Noel Briscoe
Judith Starr	Marlene Horne-Richards	Tod Ware
Israel Goldowitz	Steve Block	Anand Kothari
Ted Winter	Patricia Davis	Samuel Norfleet
Marty Boehm	Andrea Schneider	Bennie Hagans
John Greenburg	Margaret Hamilton	Candace Campbell
Walt Luiza	Ken Oliver	Michelle Gray
Wayne McKinnon	Srividhya Shyamsunder	Catherine Hammaker

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2009 and 2008 Financial Statements

Audit Report AUD-2010-2 / FA-09-64-2

Contents

Section I: Independent Auditor's Report

Section II: Management Comments

Acronyms

C&A	Certification and Accreditation
CFS	Consolidated Financial System
COOP	Continuity of Operations Program
EDM	Enterprise Data Model
ELAN	Enterprise Local Area Network
FIPS PUB	Federal Information Processing Standards Publication
FMFIA	Federal Managers' Financial Integrity Act of 1982
FY	Fiscal Year
IAH	Information Assurance Handbook
IPVFB	Integrated Present Value of Future Benefits
ISO	Information System Owner
IT	Information Technology
NIST SP	National Institute of Standards and Technology Special Publication
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAS	Premium Accounting System
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
PPS	Premium and Practitioner System
PRISM	Participant Records Information Systems Management
RTM	Requirements Traceability Matrix
TAS	Trust Accounting System

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2009 and 2008 Financial Statements

Audit Report AUD-2010-2 / FA-09-64-2

Section I

Independent Auditor's Report

Pension Benefit Guaranty Corporation

To the Board of Directors, Management,
and Inspector General of the
Pension Benefit Guaranty Corporation
Washington, DC

We have audited the financial statements of the Pension Benefit Guaranty Corporation (PBGC) as of and for the year ended September 30, 2009, and have examined management's assertion included in PBGC's Annual Management Report about the effectiveness of the internal control over financial reporting (including safeguarding assets) and PBGC's compliance with certain provisions of laws, regulations, and other matters, and have issued our combined report thereon dated November 12, 2009 (see OIG report AUD-2010-1/FA-09-64-1).

We conducted our audit and examination in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*, issued by the Comptroller General of the United States; attestation standards established by the American Institute of Certified Public Accountants; and OMB audit guidance.

The purpose of this report is to provide more detailed discussions of the specifics underlying the material weakness reported in the internal control section of our combined report on PBGC's fiscal year (FY) 2009 financial statements. As reported in our combined report on PBGC's FY 2009 financial statements, we identified certain deficiencies in internal control that we consider significant deficiencies, which combined constitute a material weakness.

Summary

PBGC protects the pensions of approximately 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, 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.

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.

As noted in FY 2008 and previous financial statement audit reports, 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 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. Integrated financial management systems

Detailed findings and recommendations follow.

In FY 2009, PBGC incorrectly reported progress in addressing weaknesses noted in its entity-wide information security management program to correct systemic security control weaknesses at the root cause level. The incorrect reporting in PBGC's status report impacted strategic decisions to prioritize resources for resolving deficiencies in PBGC's IT infrastructure. PBGC has initiated efforts in the reorganization and improvement of its security planning and management through the design and implementation of a more coherent strategy to managing its information systems. However, these efforts are not completed and additional time is needed for further strategy development and implementation.

1. Entity-wide Security Program Planning and Management

During FY 2009, PBGC incorrectly reported progress in addressing entity-wide security management weaknesses, which did not agree with its own assessment of the state of its IT infrastructure and environment. PBGC's assessment of its IT infrastructure and environment noted fundamental weaknesses in its architecture and design that prohibited the implementation of effective controls. Communication between PBGC's key decision makers did not convey the urgent need for decisive strategic decisions to correct weaknesses in PBGC's IT infrastructure and environment. Resources were inappropriately allocated to address control weaknesses that could not be resolved until fundamental IT architecture and design issues have been mitigated. The sixty-five (65) common security controls PBGC previously identified and documented, could not be implemented, despite PBGC's reporting that they have implemented forty-five (45) of them. Furthermore, PBGC was unable to complete the certification and accreditation (C&A) of thirteen (13) major applications and general support systems, although management reported the C&As were completed. PBGC's quality control review of the C&A packages did not correct specific issues we identified in FY 2008. The C&A packages were deficient in their quality, accuracy, and consistency. PBGC has not updated its Information Assurance Handbook (IAH) to reflect changes in its IT policies and procedures. Consequently, management's objective to resolve prior year control weaknesses was not achieved.

PBGC's entity-wide security program lacks focus and a coordinated effort to adequately resolve control deficiencies. These deficiencies prevent PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. The specific weaknesses we found that contributed to the material weakness and our recommendations to correct them are as follows:

- PBGC has identified sixty-five (65) common security controls for the seventeen (17) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, 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. 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.

Recommendations:

- 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)**
- Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. **(OIG Control Number FS-08-01)**
- 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)**
- PBGC's process for the completion of C&A packages in accordance with NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* 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. In FY 2009, PBGC asserted to have completed 13 C&A packages for its major applications and general support systems. Significant deficiencies noted in access controls and configuration management do not support this assertion.

PBGC's quality control review of the C&A packages did not correct specific issues we identified in FY 2008. In addition, PBGC's oversight of contractor performance during the C&A process was inadequate. The C&A packages were deficient in their quality, accuracy, and consistency.

Our review of C&A packages noted the following quality control weaknesses, each of which had been identified in our prior year audit:

- Limited documentation of test results, a condition that prevented third-party reviewers from re-performing, and thus validating, the tests.
- Deficiencies not included in the Plan of Action & Milestones.
- Documentation that did not support conclusions reached or test results.
- Inconsistencies or apparent errors and/or omissions in work performed.
- Information in the system boundaries section of the risk assessment conflicted with the listing of external connections.
- Minor applications identified in Security Control Worksheet, but not documented in the Risk Assessment.

Management provided three conflicting inventory lists of major applications and general support systems. Some systems considered major on one inventory list, were considered minor on the others. We could not determine management's assertion concerning the inventory of its major applications and general support systems. Because of the contradictory information provided, we could not determine which of these lists

should be considered as management's assertion concerning the inventory of its major applications and general support systems. Therefore, we could not determine which major applications and general support systems require certification and accreditation.

Without management oversight and accountability of contractor's performance, management may accept work that does not meet Federal criteria. Such practices may lead to fraud, waste, or abuse, and to insufficient protection of sensitive or critical resources. In addition, projects may exceed approved budget if rework is required. Without monitoring contractor performance and performing a quality review of deliverables, management cannot have confidence in the work performed.

The risk exists that systems could be certified, accredited, and receive an authorization to operate without the assurance that complete and accurate results are obtained in executing the C&A process. In addition, issues identified or missed because of inaccurate or incomplete work performed will impact the corrective action required along with the resource commitment needed to complete the intended action.

PBGC will not have reasonable assurance regarding the confidentiality, integrity, and availability of its information systems.

Recommendations:

- Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies. **(OIG Control Number FS-09-03)**
- Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control Number FS-09-04)**
- Implement an effective review process to validate the completion of the certification and accreditation 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 Number FS-08-02)**
- 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)**
- 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)**

- 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)**
- 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)**
- 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)**
- 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 Number FS-09-09)**
- 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)**
- 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)**
- Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for Security Awareness training. PBGC currently has a cumbersome and error-prone manual process to account for personnel who have completed security awareness training. The process is ineffective and limits PBGC's ability to ensure that all required personnel have completed security awareness training. In FY 2008, PBGC developed role-based training programs to disseminate its Information Assurance Handbook (IAH) policies and procedures to information system owners (ISOs), system administrators, and project managers. During our FY 2009 review, we noted that PBGC could not verify and validate whether all required personnel have completed the Information Security Awareness and Training. Some project managers, ISOs and system administrators did not attend the risk management role-based training. The Contingency Plan Specialist was not aware of IAH guidance on required annual contingency training. Fifteen (15) PBGC officials with Continuity of Operations Program (COOP) responsibilities did not attend required annual contingency training.

Lack of security awareness can lead to increased risk of security breaches and exposure to fraud. Controls may not be placed in operation as mandated by PBGC policies.

Recommendation:

- 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)**

- Office of IT (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.

Recommendation:

- 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)**

2. Access Controls and Configuration Management

Although access controls and configuration management controls are an integral part of an effective information security management program, access controls remain a systemic problem throughout PBGC. PBGC's decentralized approach to system development, system deployments, and configuration management has created an environment that lacks a cohesive structure in which to implement controls and best practices. Weaknesses in the IT environment contributed significantly to deficiencies in system configuration, segregation of duties, role-based access controls, and monitoring. Furthermore, PBGC's information systems are overlapping and duplicative, employing obsolete and antiquated technologies that are costly to maintain. The state of PBGC's IT environment led to increased IT staffing needs, manual workarounds, reconciliations, extensive manipulation, and excessive manual processing that have been ineffective in providing adequate compensating controls to mitigate system control weaknesses. For example, the Financial Reporting and Account Analysis Group manually records present value of future benefits liabilities for single employer and multiemployer programs in CFS, and the Financial Operations Department manually records Premiums Income, Premiums Receivable, and Unearned Premiums in CFS.

Access controls should be in place to consistently limit, detect inappropriate access to computer resources (data, equipment, and facilities), or monitor access to computer programs, data, equipment, and facilities. These controls protect against unauthorized modification, disclosure, loss, or impairment. Such controls include both logical and physical security controls to ensure that Federal employees and contractors will be given only the access privileges necessary to perform business functions. Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum access controls for Federal systems. FIPS PUB 200 requires PBGC's information system owners to limit information system access to authorized users.

Industry best practices, NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, and other Federal guidance recognize the importance of configuration management when developing and maintaining a system or network. Through configuration management, the composition of a system is formally defined and tracked to ensure that an unauthorized change is not introduced. Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system, on an ongoing basis, is an essential aspect of maintaining the security posture. An effective entity-wide configuration management and control policy and associated procedures are essential

to ensuring adequate consideration of the potential security impact of specific changes to an information system. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the entity and subsequently controlling and maintaining an accurate inventory of any changes to the system.

Inappropriate access and configuration management controls do not provide PBGC with sufficient assurance that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

The specific weaknesses we found that contributed to the material weakness and our recommendations to correct them are as follows:

- PBGC's configuration management controls are labor intensive and ineffective. Weaknesses in the design of PBGC's infrastructure and deployment strategy for systems and applications created an environment where strong technical controls and best practices cannot be effectively implemented. Configuration management controls are therefore not consistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server configurations; therefore, management cannot rely on results obtained in the development or test environments prior to deployment in production. Overall, the PBGC environment suffers from inadequate configuration, roles, privileges, logging, monitoring, file permissions, and operating system access.

PBGC's infrastructure does not adequately segregate the production, development and testing environments. The current environment does not provide adequate controls in which to implement an effective application development and change control program.

Significant weaknesses noted in configuration management include the following:

- Sensitive program scripts and utilities, open directories, and unsafe services accounts were not restricted.
- Unnecessary network services and duplicate groups with privileged system access were not removed.
- Not all security patches for Linux servers were installed.
- Baseline security reports were not being created and reviewed.
- Critical files, directories, and permissions were of inappropriate configuration/ownership.
- The root account could be logged into from multiple virtual consoles.
- The Premium Accounting System (PAS) resided on a database version that is unsupported. Software versions no longer supported by the vendor, increased the likelihood that new security vulnerabilities would be introduced and PBGC would not be able to mitigate the vulnerabilities.
- The hardware in place slated for disaster recovery operations of the Oracle database environment was a single server configuration lacking the Central Processing Unit and memory to maintain business functionality in the case of a total system failure to the existing headquarters data center. Furthermore, the method in which database replication was taking place from headquarters to the COOP installation is lacking in

- functionality and completeness, and would require a significant amount of subject matter expert manual intervention, in the event of an actual system failure.
- The production PBGC databases were operating on obsolete hardware at both the server and storage area network layers. The hardware supporting the Oracle database infrastructure has recently been identified by PBGC personnel as being outdated, with the production of parts no longer occurring. The infrastructure housing the production Oracle databases was actually found to demonstrate an unsupported level of 75% at the host server level. The operating systems for these servers have reached the end of service life phase 2, with minimal support being provided.
 - Developers had access to sensitive information in production by having direct development access to production systems via a database link.
 - Development and test databases have database links directly connected to the production database. This configuration of database links produces an inefficient, difficult to manage, non-scalable Oracle database solution.
 - PBGC's *storage area network* system was obsolete. There are no new hard drives being manufactured for the Sun 9980 systems in place for production database storage.
 - The IT System Life Cycle Methodology is not consistently implemented across all projects within PBGC. We reviewed the Product Quality Assurance audit summary of the HP Service Manager 7 software implementation and noted that various critical components were lacking such as:
 - Weaknesses were noted in the approval, configuration management and change control processes.
 - Failure to obtain approval signatures on key documents and test artifacts.
 - Incomplete Requirements Traceability Matrix (RTM).
 - Failure to update the RTM resulting in lack of traceability between the requirements and the test cases.
 - Lack of evidence that key test activities were conducted in the test environment as planned.
 - Backout plans for reversing system changes in case of an unexpected situation, is not consistently documented.

Controls are not in place to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected. Applications and critical business processes may not be restored in a timely manner in the event of a true disaster.

Recommendations:

- Develop and implement procedures and processes for the consistent implementation of common configuration management controls to minimize security weaknesses in general support systems. **(OIG Control Number FS-07-07)**
- Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control Number FS-09-12)**

- Establish baseline configuration standards for all of PBGC's systems. **(OIG Control Number FS-09-13)**
- Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control Number FS-09-14)**
- Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance. **(OIG Control Number FS-09-15)**
- Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control Number FS-09-16)**
- 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. PBGC reduced the number of unnecessary and generic accounts in FY 2009, but this deficiency remains a security risk.

Failure to identify and remove unnecessary accounts from the system could result in PBGC's systems being at an increased risk of unauthorized access/modification/deletion of sensitive system and/or participant information.

Recommendation:

- Continue to remove unnecessary user and/or generic accounts. **(OIG Control Number FS-07-08)**
- 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. PBGC's decentralized approach to system development and configuration management has exacerbated inconsistency and control weaknesses in implementing strong technical controls to enforce segregation of incompatible duties.

Incompatible duties and improper password management increases the potential risk of fraud, errors and omissions.

Recommendations:

- Consistently implement controls to appropriately segregate duties and grant rights and privileges commensurate with the job functions and responsibilities. **(OIG Control Number FS-07-09)**

- Assess the risk associated with 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)**
- Developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of the application, the circumvention of critical controls, and unnecessary access to sensitive data. Weaknesses in the design of PBGC's infrastructure and deployment strategy for legacy systems and applications created an environment where developers have unrestricted access to production. PBGC has not developed and implemented adequate compensating controls to restrict developer's access to production. PBGC has not fully resolved infrastructure design issues, and developed and implemented a coherent program to manage and maintain legacy applications.

Failure to appropriately restrict privileged access to the production environment could result in unauthorized access/modification/deletion to sensitive system and/or participant information and the release of harmful code into the production environment.

Recommendations:

- Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control Number FS-07-10)**
- 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)**
- 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.

Failure to follow secure build standards and reassign or remove unowned user files provides internal and external attackers additional paths into PBGC's systems and could result in an increased risk of unauthorized access, modification, or deletion of sensitive system and participant information. These control weaknesses increase the risk for fraud, waste and abuse.

Recommendations:

- Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications are in compliance with the IAH. **(OIG Control Number FS-07-11)**

- Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control Number FS-09-19)**
- 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. PBGC's configuration management weaknesses have contributed significantly to its inability to effectively implement controls to ensure the consistent removal and locking out of generic or dormant accounts.

Without full development and implementation of security controls, the lack of an effective policy addressing lock out, inactive accounts, and dormant accounts provides another control weakness that could be exploited and compromise the integrity, confidentiality and availability of PBGC's systems and applications.

Recommendation:

- 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)**
- 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 recertified annually. PBGC's infrastructure design and configuration management weaknesses have contributed significantly to its inability to effectively implement controls to recertify all user and system accounts.

Unauthorized users could gain access to PBGC's data and personally identifiable information (PII). Without periodic recertification of accounts (user, generic, service and system) management does not have adequate assurance that only current authorized users have access to PBGC resources.

Recommendation:

- 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)**
- Vulnerabilities found in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. These PBGC system vulnerabilities are caused by an ineffective deployment strategy in the development, test, and production environments. Ineffective system deployments have resulted in an environment that is in disarray.

Security control weaknesses and vulnerabilities in key databases are not mitigated, which adversely impacts the security and integrity of PBGC's development, test, and

production environments. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur, undetected.

Recommendations:

- Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control Number FS-07-14)**
- Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control Number FS-09-20)**
- 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.

Failure to ensure proper authorization may expose PBGC's systems to inadequate segregation of incompatible duties and unauthorized users having access to PBGC data and PII.

Recommendation:

- 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)**
- 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.

Without full development and implementation, security controls are inadequate to prevent contractors from having unauthorized access to PBGC's systems, applications, and facilities.

Recommendations:

- Update and enforce directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. **(OIG Control Number FS-07-16)**
- 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 IT 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.

Controls are not in place to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur, undetected.

Recommendation:

- 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)**

3. Integrated Financial Management Systems

The risk of inaccurate, inconsistent, and redundant data is increased because PBGC lacks a single integrated financial management system. The current system cannot be readily accessed and used by financial and program managers without extensive manipulation, excessive manual processing, and inefficient balancing of reports to reconcile disbursements, collections, and general ledger data.

OMB Circular A-127, *Financial Management Systems*, requires that Federal financial management systems be designed to provide for effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the systems. This Circular states:

The term "single, integrated financial management system" means a unified set of financial systems and the financial portions of mixed systems encompassing the software, hardware, personnel, processes (manual and automated), procedures, controls and data necessary to carry out financial management functions, manage financial operations of the agency and report on the agency's financial status to central agencies, Congress and the public. Unified means that the systems are planned for and managed together, operated in an integrated fashion, and linked together electronically in an efficient and effective manner to provide agency-wide financial system support necessary to carry out the agency's mission and support the agency's financial management needs.

OMB's Office of Federal Financial Management, formerly the Joint Financial Management Improvement Program, Core Financial System Requirements document, lists the following integrated financial management system attributes:

- Standard data classifications (definition and formats) established and used for recording financial events.
- Common processes used for processing similar kinds of transactions.
- Internal controls over data entry, transaction processing, and reporting applied consistently.
- A system design that eliminates unnecessary duplication of transaction entry.

Because PBGC has not integrated its financial systems, PBGC's ability to accurately and efficiently accumulate and summarize information required for internal and external financial reporting is impacted. Many of the weaknesses included in this report were reported in prior years. The specific weaknesses we found that contributed to the material weakness and our recommendations to correct them are as follows:

Lack of standard data classifications and common data elements:

- PBGC management has indicated that a logical database model (Enterprise Data Model (EDM)) has been developed and is being revised. Elements of the EDM include the general ledger, purchases, portfolio management, payroll, investment management, financial institutions, budgeting, accounts receivable, and accounts payable. Until the development and implementation of the EDM is complete, the current systems have no centralized data catalog defining data elements or a common data access method available for current databases.
- The current decentralized database structure may lead to erroneous financial and participant data. For example, the same data elements are required to be reformatted or are used for different purposes across PBGC's various applications.
- The current decentralized database structure may lead to outdated financial or participant data. Because participant data must be reformatted and distributed to multiple PBGC systems, users may be relying on outdated information to make business decisions.

Duplication of transaction entry:

- Probable and multi-employer plan data initially entered into IPVFB must be manually re-entered into a spreadsheet and then manually entered into CFS as adjusting journal entries.
- Plan data initially entered into the Case Management System application must be re-entered into the TAS application's portfolio header.
- Plan contingency listings are determined using data extracted from PAS. However, plans with multiple filings must be manually aggregated before the plans can be classified.
- Plan sponsor data address information must be manually entered into CFS to process refunds.

Obsolete and antiquated technologies:

PBGC's information systems employ obsolete and antiquated technologies that pose additional risk to the availability of financially significant systems. These technologies are unsupported and add to the challenges to integrate PBGC's systems in an IT infrastructure that lacks a cohesive architecture and design.

A Federal agency's ability to effectively and efficiently maintain and modernize its existing IT environment depends primarily on how well it employs certain IT management controls that are embodied in statutory requirements, Federal guidance, and best practices. Among other things, these controls include strategic planning and performance measurement, portfolio-based investment management, human capital management, enterprise architecture (and supporting segment architecture) development and use, and responsibility and accountability for modernization management.

If managed effectively, IT investments can have a dramatic impact on an organization's performance and accountability. If not correctly managed, they can result in wasteful spending and lost opportunities for achieving mission goals and improving mission performance. PBGC has had several false starts in modernizing its systems and applications that have either been abandoned, such as the suspension of work on the PPS to replace PAS, or have been ineffective in leading to the integration of its financially significant systems. Unless PBGC develops and implement a well designed IT architecture and infrastructure to guide and constrain modernization projects, it risks investing time and resources in systems that do not reflect the Corporation's priorities, are not well integrated, are potentially duplicative, and do not optimally support mission operations and performance.

To its credit, PBGC has begun to develop an overall strategy, but much work remains before the strategy can be completed and implemented. Steps PBGC has taken include the following:

1. PBGC has completed the identification of all systems that provide data required to prepare the financial statements.
2. PBGC has substantially completed the logical database model including standard data definitions and formats to be used throughout the Corporation.
3. PBGC has completed the development of segment architectures for CFS and Premium Accounting. Segment Architectures will assist PBGC in identifying and planning financial technology recommendations for implementation and alternative analysis for business cases.

Major work remains to be completed to set the foundation for an integrated financial management system, including the following:

1. Incorporating the results of PBGC's Sourcing and Oracle Assessments in the Segment Architecture to support the selection of best alternative for PBGC'S new IT infrastructure.
2. Completing Segment Architectures for all PBGC Architecture Segments.
3. Mapping all legacy systems to PBGC's logical database model and identifying discrepancies.
4. Developing business cases for CFS and Premium Accounting IT Investments to support budget request for system development.
5. Developing and implementing new IT system solutions/functions in accordance with the Financial Management Segment Architecture and strategic system plan.
6. Completing alternative analysis studies for CFS and Premium Accounting.

Recommendation:

- o PBGC needs to develop and execute a plan to integrate its financial management systems in accordance with OMB Circular A-127. **(OIG Control Number FS-07-18)**

The status of the internal control report recommendations is presented in Exhibit I.

This report is intended for the information and use of the management and Inspector General of PBGC and is not intended to be and should not be used by anyone other than these specified parties.

Clifton Henderson LLP

Calverton, Maryland
November 12, 2009

EXHIBIT I - Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendations Closed During FY 2009:

Recommendation	Date Closed	Original Report Number
FS-08-04	10/27/2009	AUD-2009-2/FA-08-49-2
FS-08-05	10/27/2009	AUD-2009-2/FA-08-49-2

Open Recommendations as of September 30, 2009:

Recommendation	Report
<u>Prior Years'</u>	
FS-07-04	2008-2/FA-0034-2
FS-07-06	2008-2/FA-0034-2
FS-07-07	2008-2/FA-0034-2
FS-07-08	2008-2/FA-0034-2
FS-07-09	2008-2/FA-0034-2
FS-07-10	2008-2/FA-0034-2
FS-07-11	2008-2/FA-0034-2
FS-07-12	2008-2/FA-0034-2
FS-07-13	2008-2/FA-0034-2
FS-07-14	2008-2/FA-0034-2
FS-07-15	2008-2/FA-0034-2
FS-07-16	2008-2/FA-0034-2
FS-07-17	2008-2/FA-0034-2
FS-07-18	2008-2/FA-0034-2
FS-08-01	AUD-2009-2/FA-08-49-2
FS-08-02	AUD-2009-2/FA-08-49-2
FS-08-03	AUD-2009-2/FA-08-49-2
<u>FY Ended September 30, 2009</u>	
FS-09-01	AUD-2010-2/FA-09-64-2
FS-09-02	AUD-2010-2/FA-09-64-2
FS-09-03	AUD-2010-2/FA-09-64-2
FS-09-04	AUD-2010-2/FA-09-64-2
FS-09-05	AUD-2010-2/FA-09-64-2
FS-09-06	AUD-2010-2/FA-09-64-2
FS-09-07	AUD-2010-2/FA-09-64-2
FS-09-08	AUD-2010-2/FA-09-64-2
FS-09-09	AUD-2010-2/FA-09-64-2
FS-09-10	AUD-2010-2/FA-09-64-2
FS-09-11	AUD-2010-2/FA-09-64-2
FS-09-12	AUD-2010-2/FA-09-64-2
FS-09-13	AUD-2010-2/FA-09-64-2
FS-09-14	AUD-2010-2/FA-09-64-2
FS-09-15	AUD-2010-2/FA-09-64-2
FS-09-16	AUD-2010-2/FA-09-64-2
FS-09-17	AUD-2010-2/FA-09-64-2
FS-09-18	AUD-2010-2/FA-09-64-2
FS-09-19	AUD-2010-2/FA-09-64-2
FS-09-20	AUD-2010-2/FA-09-64-2

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2009 and 2008 Financial Statements

Audit Report AUD-2010-2 / FA-09-64-2

Section II

Management Comments



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

Office of the Director

MEMORANDUM

November 12, 2009

To: Rebecca Anne Batts
Inspector General

From: Vincent K. Snowbarger
Acting Director

Subject: Response to the Office of Inspector General's (OIG's) Draft
Opinion on Internal Controls for FY 2009

Thank you for the opportunity to respond to the subject draft report. PBGC is committed to addressing the recommendations contained in this report and to remediating the associated material weakness. Management's own internal review process has largely corroborated the findings in this year's audit, and I have accordingly increased management oversight of the Information Technology (IT) operational area. Of the 37 recommendations in the draft report on internal controls, 27 recommendations remain open from prior audit findings with which management has already agreed, and we reiterate that agreement below. We also agree with the 10 new recommendations. Thus, there are no reported recommendations requiring resolution under Office of Management and Budget (OMB) Circular A-50.

We have provided our responses to each recommendation below, and we will be preparing top-level corrective action plans (CAPs) in the near future, with additional specificity following that. New management has only recently been installed over our IT operations, which are central to the development and execution of upgraded and realistic corrective action plans for most of the reported recommendations. As a result, over the next several months, we expect to make changes in the priority and scheduling of specific recommendations. We will keep your office informed of these developments. Overall, we anticipate that addressing these recommendations will require at least three years of concerted effort, though I expect to see substantive progress in every year moving forward.

The efforts of your office that went into preparing this detailed report are sincerely appreciated, and management also appreciates the need to work together as we address the noted issues.

Entity-wide Security Program Planning and Management

1. **Recommendation:** 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)**

Response: Management agrees. We would, in fact take the findings a step further. Communication to key decision-makers did not convey the urgent need for decisive strategic decisions and actions to correct fundamental weaknesses in PBGC's IT controls and security. Further, in management's view, resources were inappropriately allocated, not simply because they were put to control weaknesses that "could not be resolved until fundamental IT architecture and design issues have been mitigated," as the draft report has it, but even more significantly, because the approaches taken did not address the fundamental problems and did not include effective interim controls to mitigate risk and afford management the ability to address fundamental problems over the long term. This audit, corroborated by management's own work under the Contracts and Controls Review Department, has helped to effect that communication. As a result, management has taken appropriate actions to begin the remediation process.

2. Recommendation: Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified. **(OIG Control Number FS-08-01)**

Response: Management agrees. Management has itself tested the 65 common security controls over the past two years and has made measured progress, though much remains to be done.

3. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 2, above.

4. Recommendation: 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)**

Response: Management agrees. Management is committed to addressing the security issues noted here and in Recommendations 5 and 18, and we will formulate a CAP with these in mind, to facilitate interim control needs and long-term IT effectiveness.

5. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 4, above.

6. Recommendation: Implement an effective review process to validate the completion of the certification and accreditation 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 Number FS-08-02)**

Response: Management agrees. We are implementing a more rigorous review process to ensure that future information provided is as accurate and reliable as possible.

7. Recommendation: 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)**

Response: Management agrees. We are validating the current inventory of our major applications and general support systems. In addition, we will implement a repeatable process to control the accuracy of this inventory to include all Certification and Accreditation (C&A)-related artifacts.

8. Recommendation: 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)**

Response: Management agrees. We are fully committed to establishing and implementing comprehensive procedures that document the roles and responsibilities that ensure oversight and accountability in the certification and review process. We will also retain evidence of oversight reviews and take appropriate action to address erroneous or unsupported reports of progress.

9. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 7, above.

10. Recommendation: 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)**

Response: Management agrees. As part of our CAP, we will review and improve our C&A processes, roles, and responsibilities to ensure that the C&As have integrity.

11. Recommendation: 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)**

Response: Management agrees. We have begun to initiate steps to rectify the condition cited, and we will develop and implement a CAP to fully address the issues associated with the C&A process, as well as the related contractor oversight.

12. Recommendation: 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 Number FS-09-09)**

Response: Management agrees. Please see the response to Recommendation 11, above.

13. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 11, above.

14. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 11, above.

15. Recommendation: 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)**

Response: Management agrees. We will identify the various roles and the related required training, and we will develop and follow a disciplined approach to ensuring the required training is received timely as part of our overall CAP.

16. Recommendation: 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)**

Response: Management agrees. As the audit report notes, PBGC is in the process of completing the development and distribution of measurable services that OIT provides to the business owners. Moreover, we are fully committed to the completion of this effort, as it impacts the work of the Corporation.

Access Controls and Configuration Management

17. Recommendation: 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)**

Response: Management agrees. We are working to establish a CAP that fully addresses the implementation of a sufficient configuration management program. In that effort, we will appreciate a continuing dialogue with your office regarding several of the specific conditions reported as findings in this year's report, as detailed in management's response to the related Notifications of Findings and Recommendations (NFRs), in order to gain clarification.

18. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 4, above.

19. Recommendation: Establish baseline configuration standards for all of PBGC's systems. **(OIG Control Number FS-09-13)**

Response: Management agrees. Please see the response to Recommendation 17, above.

20. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 17, above.

21. Recommendation: 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)**

Response: Management agrees. As suggested by the audit report itself, this is a complex issue, with multiple layers that need to be addressed. Management will develop a CAP that will address the findings as outlined and establish compensating controls, as needed, during the development of longer term solutions.

22. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 21, above.

23. Recommendation: Continue to remove unnecessary user and/or generic accounts. **(OIG Control Number FS-07-08)**

Response: Management agrees. We will develop and implement a CAP for establishing the Enterprise Security Program, with short-, medium-, and long-term goals. The objective of this enterprise-level CAP is to address the root causes of the auditor's Fiscal Year (FY) 2009 and prior year findings.

24. Recommendation: 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)**

Response: Management agrees. These findings, which originally arose in a prior audit, were corroborated by management's own FY 2009 assessment of our Oracle database. Management is fully committed to the development of a CAP that addresses the root causes of these findings.

25. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 24, above.

26. Recommendation: Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control Number FS-07-10)**

Response: Management agrees. Management will develop and implement a CAP that appropriately restricts developers' access to the production environment and documents any exigent access with the requisite management approval.

27. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 26, above.

28. Recommendation: 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)**

Response: Management agrees. We will develop and implement a CAP that will ensure that authentication parameters are compliant with the Information Assurance Handbook and that we periodically review systems for compliance with baseline settings.

29. Recommendation: Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control Number FS-09-19)**

Response: Management agrees. Please see the response to Recommendation 28, above.

30. Recommendation: 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)**

Response: Management agrees. We will develop and implement corrective actions that will appropriately lock out and remove inactive and dormant accounts.

31. Recommendation: 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)**

Response: Management agrees. We will complete the work that we have begun to implement the recertification process as an ongoing annual one that includes all of PBGC's accounts.

32. Recommendation: 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)**

Response: Management agrees. Management's own assessment of our Oracle environment corroborated the finding of an earlier audit report, which led to this recommendation. The recent assessment provided additional information that will be useful in addressing this issue. We are fully committed to developing a CAP that will strengthen our controls to address the cited vulnerabilities and weaknesses.

33. Recommendation: 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)**

Response: Management agrees. Please see the response to Recommendation 32, above.

34. Recommendation: 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)**

Response: Management agrees. In formulating an appropriate CAP, we would like an opportunity to meet with the auditors to review their evidence regarding incomplete ELAN forms and remote access forms. This will enable us to better target corrective actions and monitor progress.

35. Recommendation: Update and enforce directive PM 05-1, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, to ensure contract personnel can be tracked effectively. Also, ensure a formal Entrance on Duty and Separation Clearance process is followed. **(OIG Control Number FS-07-16)**

Response: Management agrees. We have assigned the appropriate departments the task of reviewing and revising the related CAP to ensure that this issue is addressed.

36. Recommendation: 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)**

Response: Management agrees. Management's own assessment of our Oracle database here again corroborated an earlier related audit finding. We are committed to developing and implementing a CAP that addresses this finding.

37. Recommendation: PBGC needs to develop and execute a plan to integrate its financial management systems in accordance with OMB Circular A-127. **(OIG Control Number FS-07-18)**

Response: Management agrees. We appreciate the acknowledgement in the audit report of steps that we have taken to move towards the more complete integration of our financial management systems. We are committed to developing and acting upon a broader, cost-effective CAP that will more fully integrate our systems in accordance with OMB Circular A-127.

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