Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2011 and 2010 Financial Statements Audit

November 14, 2011

AUD 2012-2/FA-11-82-2

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

November 14, 2011

To: Josh Gotbuam
Director

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 2011 and 2010 Financial Statements Audit (AUD-2012-2 / FA-11-82-2)

I am pleased to transmit the attached report prepared by Clifton Gunderson LLP resulting from their audit of the PBGC Fiscal Year 2011 and 2010 Financial Statements. The purpose of this report is to provide more detailed discussions of the specifics underlying the material weaknesses and significant deficiency reported in the internal control section of the combined Independent Auditor's Report dated November 14, 2011 (AUD-2012-1 / FA-11-82-1).

The attached management response to a draft of this report indicates that PBGC is in agreement with the vast majority of findings and recommendations. Thus, we have an agree-to management decision for 44 of the 55 recommendations. However, management disagreed with five recommendations addressing information technology control weaknesses relating to PBGC's contract service providers, including three recommendations dealing with a Security Operations Center located outside of the United States. For six additional recommendations addressing weaknesses in the Benefits Administration and Payment Department, PBGC management agreed with the recommendations and committed to addressing the issue through a corrective action plan. While management's response to the six recommendations is positive, it does not provide enough detail for us to determine whether we can agree with PBGC's management decision. We will work with the Corporation in the coming weeks to resolve these issues and reach an agreed-to management decision for each of the remaining eleven recommendations.

We would like to take this opportunity to express our appreciation for the cooperation that was provided during the performance of the audit.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2011 and 2010 Financial Statements

Audit Report AUD-2012-2 / FA-11-82-2

Contents

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2011 and 2010 Financial Statements

Audit Report AUD-2012-2 / FA-11-82-2

Acronyms

A&A	Assessment and Authorization
BAPD	Benefits and Payment Department
CAP	Corrective Action Plan
CFS	Consolidated Financial System
CMS	Case Management System
COOP	Continuity of Operations Program
DoPT	Date of Plan Termination
EDM	Enterprise Data Model
FIPS PUB	Federal Information Processing Standards Publication
FY	Fiscal Year
IAH	Information Assurance Handbook
IPERA	Improper Payments Elimination and Recovery Act
IPVFB	Integrated Present Value of Future Benefits
ISA	Interconnection Security Agreement
IT	Information Technology
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OFFM	OMB Office of Federal Financial Management
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAM	Portfolio Accounting and Management
PAS	Premium Accounting System
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
PLUS	Pension Lump Sum System
PRISM	Participant Records Information Systems Management
RTM	Requirements Traceability Matrix
SOC	Security Operations Center
SP	Special Publication
TAS	Trust Accounting System

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2011 and 2010 Financial Statements

Audit Report AUD-2012-2 / FA-11-82-2

Section I

Independent Auditor's Report

Clifton Gunderson LLP
Certified Public Accountants & Consultants

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 or the Corporation) as of and for the year ended September 30, 2011, and have examined management's assertion included in PBGC's Annual 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 14, 2011 (see Office of Inspector General (OIG) report AUD-2012-1/FA-11-82-1).

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 Office of Management and Budget (OMB) audit guidance.

The purpose of this report is to provide more detailed discussions of the specifics underlying the material weaknesses reported in the internal control section of our combined report on PBGC's fiscal year (FY) 2011 financial statements. As reported in our combined report on PBGC's FY 2011 financial statements, we identified certain deficiencies in internal control that we consider material weaknesses, and other deficiencies that we consider to be a significant deficiency.

Summary

PBGC protects the pensions of approximately 44 million workers and retirees in more than 27 thousand private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on information technology (IT) and the effective operation of the Benefits Administration and Payment Department (BAPD). 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.

11710 Beltsville Drive, Suite 300
Calverton, MD 20705-3106
tel: 301-931-2050
fax: 301-931-1710

www.cliftoncpa.com

The slow progress of mitigating PBGC's systemic security control weaknesses and the serious internal control weaknesses in BAPD posed an increasing and substantial risk to PBGC's ability to carry out its mission during FY 2011. The extended time required and the lack of meaningful progress in PBGC's multi-year approach to correct previously reported deficiencies at the root cause level, introduced additional risks. These include technological obsolescence, inability to execute corrective actions, breakdown in communications and poor monitoring. BAPD's weak internal controls create an environment that could lead to fraud, waste, and abuse.

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

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

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

We continued to find deficiencies in the areas of security management, access controls, configuration management, and segregation of duties. Control deficiencies were also found in policy administration and the A&As.

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 its security posture. This framework will require time for effective control processes to mature.

Additionally, serious internal control weaknesses in BAPD's operations were identified by the Office of the Inspector General (OIG) and others during FY 2011. These significant control weaknesses introduced additional risks to PBGC. Specific deficiencies included errors in valuation of plan assets, lack of documentation supporting benefit payments, errors in benefit calculations, and poor oversight of the Pension and Lump Sum System (PLUS). In response to weaknesses identified by OIG, BAPD is currently undergoing a strategic review that may address organizational structure and operational issues. BAPD stated it will develop a plan in FY 2012 that will address the deficiencies noted in the financial statement audit, Improper Payments Elimination and Recovery Act (IPERA) mandated review, and other internal reviews. This plan is intended to focus on fundamental issues such as internal controls, processes, contractor oversight, and training and staff competencies.

Based on our findings, we are reporting that the deficiencies in the following areas constitute three material weaknesses for FY 2011:

1. Entity-wide Security Program Planning and Management
2. Access Controls and Configuration Management
3. Benefits Administration and Payment Department Operations

We are also reporting the deficiencies in the following area to be a significant deficiency for FY 2011:

4. Integrated Financial Management Systems

Detailed findings and recommendations follow.

1. Entity-wide Security Program Planning and Management

An entity-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall policies and plans are developed at the entity-wide level. System and application-specific procedures and controls implement the entity-wide policy. Through the Federal Information Security Management Act of 2002, Congress requires each Federal agency to establish an agency-wide information security program to provide security to the information and information systems that support the operations and assets of the agency, including those managed by a contractor or other agency. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources,* requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

PBGC continued the implementation of its CAP to address fundamental weaknesses in its entity-wide security program planning and management. During FY 2011, PBGC began the implementation of a more rigorous and thorough A&A process. Through this process, PBGC identified significant fundamental security control weaknesses for its general support systems, many of which were reported on in prior years' audits. While this is an important step in the planning process, these security control weaknesses remain unresolved and PBGC's efforts lack sufficient meaningful incremental progress. PBGC reports that they are in the process of performing A&As on its major applications. The slow rate of progress has introduced additional risks including technological obsolescence, inability to execute corrective actions, breakdown in communications and poor monitoring.

In prior years, PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. These deficiencies, which persisted throughout FY 2011, prevented PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. Without a well-designed and fully implemented information security management program, there is increased risk that security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions may lead

to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

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

- PBGC had not completed A&As for any major applications.

- PBGC had not completed A&As for the general support systems hosted by third party processors on behalf of PBGC.

- National Institute of Standards and Technology (NIST) special publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* identifies 172 controls within 17 security control families. PBGC identified 130 of these controls as their common security controls. While PBGC has stated they anticipate completion of the CAP in early 2015, as of the end of FY 2011, they have not documented the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of these identified common security controls,

- Weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications adversely affected its ability to effectively implement common security controls across its systems and applications. Without full development and implementation, security controls are inadequate; responsibilities are unclear, misunderstood, and improperly implemented; and controls are inconsistently applied. Such conditions lead to insufficient protection of sensitive or critical resources or disproportionately high expenditures for controls. Consequently, as PBGC had not completed and confirmed the design, implementation, and operating effectiveness of its common security controls, 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 # FS-09-01)**

  - Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 130 identified common security controls. **(OIG Control # FS-08-01 *Modified)**[1]

  - Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control # FS-09-02)**

  - Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies. **(OIG Control # FS-09-03)**

- Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control # FS-09-04)**

- Implement an effective review process to validate the completion of the A&A packages for all major applications. The review should not be performed by an individual associated with the performance of the A&A, or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control # FS-08-02 *Modified)**

- Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the A&A process for all major applications. **(OIG Control # FS-09-05 *Modified)**

- Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the A&A review process for major applications. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control # FS-09-06 *Modified)**

- Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC Office of IT (OIT) operations. **(OIG Control # FS-09-07)**

- Implement an independent and effective review process to validate the completion of the A&A packages for all major applications. **(OIG Control # FS-08-03 *Modified)**

- Implement an independent and effective review process to validate the completion of the A&A packages for general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control # FS-08-03 *Modified)**

- 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.

  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:

  - Continue to disseminate the awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04 *Modified)**

- In FY 2010, PBGC's benefit payments service provider (service provider) implemented a security operations center (SOC) outside of the United States (US), without providing PBGC adequate advance notice. In FY 2011, PBGC completed a risk assessment but did not contain adequate evidence to verify and validate the technical security risks of the SOC. Because the SOC has some responsibility for monitoring security-related events associated with the PLUS application and components of its system boundary, it is important PBGC assess risks to its systems and implement mitigating controls to ensure compliance with PBGC's policies and procedures.

  Recommendations:

  - Develop and implement an immediate plan of action to address the potential security risk posed by locating the SOC outside of the US. **(OIG Control # FS-10-01)**

  - Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and the Federal Information Security Management Act (FISMA). **(OIG Control #FS-10-02)**

  - Ensure that adequate controls in the design and implementation of the SOC are in place to protect PBGC PLUS. **(OIG Control Number # FS-11-01)**

- PBGC has not executed interconnection security agreements (ISA) or memorandums of understanding (MOU) between all external organizations whose systems interconnect with PBGC's systems. Controls to require such agreements do not exist.

  PBGC is in the process of planning and documenting security agreements for interconnection with all external organizations' systems. In the absence of an ISA and MOU, either party (PBGC or external system owner) may be unfamiliar with the technical requirements of the interconnection and the details that may be required to provide overall security for systems that are interconnected.

  Recommendation:

  - Develop controls and implement an ISA and MOU with all external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03 *Modified)**

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 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.

Access controls should be in place to consistently limit, detect inappropriate access to computer resources (data, equipment, and facilities), and 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 identified in prior years that contributed to the material weakness identified in FY 2011 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 in configuration management noted in prior years and continuing throughout FY 2011, included the following:

- Sensitive program scripts and utilities, open directories, and unsafe service accounts were not restricted.
- Unnecessary network services and duplicate groups with privileged system access were not removed.
- Baseline security reports were not being created and reviewed.
- Ownership of critical files, directories, and permissions were inappropriately configured.
- The root account could be logged into from multiple virtual consoles.
- The database replication from headquarters to the COOP installation is lacking in functionality and completeness, and would require a significant amount of subject matter expert manual intervention to failback to headquarters in the event of an actual system failure.
- Developers had access to sensitive information in production.
- 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 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, are 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 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 # 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 # FS-09-12)**

- Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # 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 # FS-09-14)**

- Ensure test, development and production databases are appropriately segregated to protect sensitive information and fully utilized to increase system performance. **(OIG Control # FS-09-15)**

- Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control # FS-09-16)**

- 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 has taken action to review generic accounts on the general support system, removing those that are unnecessary and approving those that are necessary, however, more work is needed to ensure that all unnecessary and generic accounts are removed. Management stated that the process for recertifying accounts will include generic accounts, service accounts, user accounts and system accounts.

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

  Recommendation:

  - Continue to remove unnecessary user and/or generic accounts. **(OIG Control # 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. Password management controls are not consistently implemented and are not standardized. PBGC's historical 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 increase the potential risk of fraud, errors and ommissions.

Recommendations:

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

- o Assess the risk associated with the lack of segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. **(OIG Control # FS-09-17 *Modified)**

- Some developers have access to the production environment, which exposes PBGC to the risk of unauthorized modification of the application, the circumvention of critical controls, and unnecessary access to sensitive data. Weaknesses in the design of PBGC's infrastructure and deployment strategy for legacy systems and applications created an 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, nor have they 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 of sensitive system and/or participant information and the release of harmful code into the production environment.

  Recommendations:

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

  - o Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed. **(OIG Control # FS-09-18)**

- Controls are not consistently applied to ensure that authentication parameters for general support systems (e.g. Novell, Windows, SUN Solaris, Oracle, etc.) and applications comply with the Information Assurance Handbook (IAH). PBGC's decentralized approach to system development and configuration management has made it particularly difficult to implement consistent technical controls across PBGC's many systems, platforms, and applications.

  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.

Recommendations:

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

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

PBGC's configuration management weaknesses have contributed significantly to its inability to effectively implement controls to ensure the consistent removal and locking out of generic or dormant accounts. The lack of controls to remove/disable inactive accounts and dormant accounts exposes PBGC's systems to exploitation and compromise.

Recommendation:

- o For the remaining systems, apply controls to remove/disable inactive and dormant accounts after a specified period in accordance with the IAH. **(OIG Control # FS-07-12 *Modified)**

- The OIT recertification process is incomplete and only addresses generic and service accounts; it does not include all user and system accounts. In addition, the Recertification of User Access Process, version 4.0, does not explicitly state that all accounts (e.g. user, system, and service) across all platforms and applications will be re-certified annually. PBGC's infrastructure design and configuration management weaknesses have contributed significantly to its inability to effectively implement controls to recertify all user and system accounts.

  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:

  - o Complete the implementation of the recertification process for all user and system accounts. Continue to perform annual recertification and include all PBGC's accounts (e.g. user, generic, service, and systems accounts) for general support systems and major applications. **(OIG Control # FS-07-13)**

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

  Security control weaknesses and vulnerabilities in key databases remain unresolved. These control weaknesses are scheduled to be corrected in 2013. These weaknesses

expose PBGC to increased risk of data modification or deletion. Unauthorized changes could occur and not be detected.

Recommendations:

- o Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control # FS-07-14)**

- o Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control # FS-09-20)**

- Access request authorizations were not appropriately documented. PBGC has not fully implemented controls to ensure Enterprise Local Area Network 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:

  - o Ensure that adequate documentation of access authorization is maintained by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control # FS-07-15)**

- PBGC lacks an effective process to track contractors throughout their employment at PBGC, including appropriate notifications of start dates and separation. PBGC updated its directive PM 05-1, PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees, in FY 2011 to provide for the effective enforcement of controls designed to track entrance and separation of all Federal and contract employees. However, the implementation PM 05-1 has not reached a level of maturity to test and validate the effectiveness of these controls. Without full implementation, security controls are inadequate to prevent contractors from having unauthorized access to PBGC's systems, applications, and facilities.

  Recommendation:

  - o 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 # FS-07-16)**

- Periodic logging and monitoring of security-related events for PBGC's applications were inadequate for CFS, Premium Accounting System (PAS), Trust Accounting System (TAS), Participant Records Information Systems Management (PRISM), and Integrated Present Value of Future Benefits (IPVFB) systems. PBGC's IT infrastructure consists of multiple legacy systems and applications (e.g. PAS, TAS, IPVFB, PRISM, etc.) that do not have a coherent architecture for management and security.

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 # FS-07-17)**

- The application virtualization/application delivery product Citrix MetaFrame Presentation Server used by PBGC's benefit payments service provider to connect to its benefit payments system, PLUS, reached its end of life date on December 31, 2009. PBGC did not include the Citrix MetaFrame Presentation Server in the system boundary when conducting the A&A of the PLUS application. Although continuous monitoring was implemented, no alerts were provided to PBGC about the application virtualization/application becoming obsolete and the potential security risk to PLUS. Obsolete software may expose PBGC's infrastructure to a security-related vulnerability. PBGC is exposed to increased risk of data modification or deletion. Unauthorized changes could occur undetected.

- Privileged TeamConnect group accounts use shared accounts to grant access to users. The activity by these privileged users cannot be tracked and/or traced to an individual user. Additionally, TeamConnect developers have access to both the development and production system. Malicious changes could be made without detection.

Recommendations:

- Replace the Citrix MetaFrame presentation server. **(OIG Control #FS-10-04)**

- Include the application virtualization/application delivery product used by the benefit payments service provider to access the PLUS application in the system boundary. **(OIG Control # FS-10-05)**

- Establish unique accounts for each user in TeamConnect. **(OIG Control Number FS-11-02)**

- Restrict developer's access to production. **(OIG Control Number FS-11-03)**

- Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs. **(OIG Control Number FS-11-04)**

- Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control Number FS-11-05)**

3. Benefits Administration and Payment Department Operations

BAPD had serious internal control weaknesses identified by OIG and others during FY 2011 that introduced additional risks to PBGC. Specific deficiencies included errors in valuation of plan assets, lack of documentation supporting benefit payments, errors in benefit calculations, and poor oversight of PLUS. In response to weaknesses identified by OIG, BAPD is currently undergoing a strategic review that may address organizational structure and operational issues. BAPD stated it will develop a plan in FY 2012 that will address the deficiencies noted in the financial statement audit, IPERA mandated review, and other internal reviews. This plan is intended to focus on fundamental issues such as internal controls, processes, contractor oversight, and training and staff competencies.

Internal control weaknesses were pervasive throughout BAPD; however many of the weaknesses identified as part of our financial statement audit stemmed from poor management of contractors. Effective oversight requires good communications with contractors on their responsibilities for contract compliance and providing timely information to PBGC that may affect the controls and/or PBGC's environment. Contracted services are an extension of PBGC's internal controls. PBGC's management does not always consider the exposure and risk that contractors introduce into its environment and how to manage that risk. PBGC does not properly review, assess, and monitor contractor's internal controls related to contracted services.

During FY 2011 we noted deficiencies in BAPD's oversight of contracted reviews of asset values at the date of plan termination (DoPT). These deficiencies were caused by a failure to establish and apply a quality review process to verify and validate the satisfactory completion of contracted DoPT plan asset valuation audits, and a failure to establish a detailed process to ensure the consistent application of a methodology to determine the fair market value of plan asset at DoPT as required by regulation. Specific deficiencies noted include the following:

- PBGC did not exercise due professional care in the conduct and oversight of contracted audits of asset values at DoPT. PBGC accepted plan asset values based on audits with audit procedures not performed or not properly documented. Audits were identified, which were accepted, that that did not meet contractual requirements to conduct the audit consistent with Generally Accepted Government Auditing Standards.

- There were instances where no corroborating evidence existed that PBGC personnel reviewed the contractors' work; however, plan asset values were approved and used in the determination of plan benefit payments and the present value of future benefits.

- PBGC has not developed a plan to ensure the proper oversight of future plan asset valuations and to ensure the identification and correction of past errors.

Recommendations:

  - Implement procedures to verify that future contracts for plan asset valuations clearly outline expectations and deliverables in the statement of work. **(OIG Control Number # FS-11-06)**

- Develop a quality assurance program aimed to ensure that plan asset valuations meet the regulatory standard of determining fair market value based on the method that most accurately reflects fair market value. **(OIG Control Number # FS-11-07)**

- Enhance and formalize efforts to improve staff skills, whether Federal or contactor, in planning the valuation reviews, understanding the risks, and developing appropriate scopes and procedures to support credible and reliable results. **(OIG Control Number # FS-11-08)**

- Identify those plans that might potentially have a pervasive misstatement to the financial statements if DOPT asset values were originally misstated. Management should then re-evaluate the DOPT asset values for those identified plans and consider the impact of any known differences on the financial statements. **(OIG Control Number # FS-11-09)**

A strong control environment is imperative to provide reasonable assurance that funds are not lost because of improper payments, whether fraudulent or erroneous. A critical element of an effective control environment includes a process to accumulate and archive documentation, including evidencing appropriate review and approval. Specific deficiencies noted include the following:

- During FY 2011 PBGC performed an IPERA mandated review which resulted in the identification of numerous instances where benefit payments were not supported by sufficient documentation necessary to verify the accuracy of the payment, and/or lacked evidence of appropriate review and approval. A statistical extrapolation of the sample results was performed and this statistical projection indicated a serious condition exists.

- In our testing of benefit calculations, we noted several instances where documents relied upon in the calculations were not archived in the Image Processing System.

Lack of appropriate documentation results in limited physical and financial controls, and could lead to improper benefit payments, as well as misunderstandings and conflicts with participants regarding the amounts and timing of their benefit payments. Best practice maintenance of source records should include a consolidation of all relevant data in a common location.

Recommendations:

- Modify the BAPD Operations Manual to explicitly incorporate policies and procedures to archive source records. The BAPD Operations Manual details the process of creating the participant database, but does not explicitly require the archival of source records. **(OIG Control Number # FS-11-10)**

- Ensure adequate documentation is maintained, which supports, substantiates, and validates benefit payment calculations by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control # FS-11-11)**

We noted deficiencies in BAPD's benefit determination process resulting in errors in calculated benefits. Specific deficiencies noted include the following:

- Testing of benefit calculations revealed instances where benefit determinations were incorrectly calculated due to errors in the application of plan provisions.

  Recommendation:

  - Improve the training of persons tasked with the calculation and review of benefit determinations to ensure their skills are matched with the complexities of the tasks assigned. **(OIG Control Number FS-11-12)**

- An MOU between PBGC and the service provider for the PLUS application was executed within PBGC between PBGC federal employees and not with the service provider. This MOU is needed to document the service provider's responsibilities and security requirements for PLUS, however, it serves no purpose since the service provider did not sign it. Further, executing the MOU between federal employees and omitting the service provider demonstrates a lack of understanding of the purpose and importance of the agreement.

  Recommendation:

  - Obtain a contract system representative signature on the PLUS MOU or alternatively, develop an interconnection security agreement (ISA) between PBGC and the benefit payments service provider for the connection. **(OIG Control Number FS-11-13)**

- PBGC did not review the service provider personnel's access to the PLUS system to ensure the personnel were appropriately recertified. PBGC relies upon the service provider to test recertification and to assert that individuals have the proper access to the system. PBGC performed no further review to test the service provider's assertion that user access is appropriate. The risk to PBGC is increased as the service provider's PLUS users typically have greater access to the PLUS system than users at PBGC.

  Recommendation:

  - Annually review contractor access recertifications for the benefit payments service provider employees with access to PLUS. **(OIG Control Number FS-11-14)**

- PBGC did not conduct a review of the PLUS System Contingency Plan until July 2011 when we requested the documentation as part of the financial statement audit. Even after receipt of the document, PBGC did not evaluate the scope of the contingency plan nor did PBGC assess the plan's compliance with NIST SP 800-34 requirements. Without a full review of the PLUS System Contingency Plan, PBGC cannot assess the adequacy of the plan and may not be able to recover from a disaster.

  Recommendation:

  - Review the PLUS contingency plan for compliance with NIST SP 800-34 requirements. **(OIG Control Number FS-11-15)**

- Our assessment of the information PBGC provided as support for assessing the risk of operating a SOC in a foreign country found that PBGC's risk assessment was not

adequate. Information relied upon included a generic overview of connectivity which did not demonstrate specifics on encryption end points, protocol filters, source and destination filters and intervening infrastructure component locations critical to the analysis of any design investigations. Without detailed network documentation of the SOC, SSC and PBGC and are unable to adequately assess the risks of the SOC implementation. Further, PBGC did not address the verification of background checks for the employees of the foreign country SOC and PBGC was unable to adequately assess the risks of the SOC implementation. Without proper background checks, PBGC may place trust in an individual who is a security risk. Without a proper assessment of the risk of a SOC implementation, PBGC may not be able to monitor or implement adequate security controls.

Recommendations:

- Develop and implement a policy to identify and document the risks associated with PBGC operations performed in foreign countries, ensure appropriate management review, and take appropriate actions to mitigate identified risks. **(OIG Control Number # FS-11-16)**

- For the PLUS SOC operating in a foreign country revise the existing risk assessment to identify and document risks, and take appropriate actions. **(OIG Control Number # FS-11-17)**

4. 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. The Circular states:

> A financial system, hereafter referred to as a core financial system, is an information system that may perform all financial functions including general ledger management, funds management, payment management, receivable management, and cost management. The core financial system is the system of record that maintains all transactions resulting from financial events. It may be integrated through a common database or interfaced electronically to meet defined data and processing requirements. The core financial system is specifically used for collecting, processing, maintaining, transmitting, and reporting data regarding financial events. Other uses include supporting financial planning, budgeting activities, and preparing financial statements. Any data transfers to the core financial system must be: traceable to the transaction source; posted to the core financial system in accordance with applicable guidance from the Federal Accounting Standards Advisory Board; and in the data format of the core financial system.

OMB's Office of Federal Financial Management (OFFM), *Core Financial System Requirements*, lists the following financial management system performance goals, outlined in the Framework document, applicable to all financial management systems. All financial management systems must do the following:

- Demonstrate compliance with accounting standards and requirements.

- Provide timely, reliable, and complete financial management information for decision making at all levels of government.

- Meet downstream information and reporting requirements with transaction processing data linked to transaction engines.

- Accept standard information integration and electronic data to and from other internal, governmentwide, or private-sector processing environments.

- Provide for "one-time" data entry and reuse of transaction data to support downstream integration, interfacing, or business and reporting requirements.

- Build security, internal controls, and accountability into processes and provide an audit trail.

- Be modular in design and built with reusability as an objective.

- Meet the needs for greater transparency and ready sharing of information.

- Scale to meet internal and external operational, reporting, and information requirements for both small and large entities.

Because PBGC has not fully 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:

<u>Lack of standard data classifications and common data elements</u>:

- PBGC continues to work towards a logical database model (Enterprise Data Model (EDM). 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 (CMS) 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 had several false starts in modernizing its systems and applications that have either been abandoned, such as the suspension of work on the Premium and Practitioner System to replace PAS, or have been ineffective in leading to the integration of its financially significant systems. Unless PBGC develops and implements 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 began to develop an overall strategy, but much work remains before the strategy can be completed and implemented. Steps PBGC has taken include the following:

- Continued work on its Enterprise Target Architecture (ETA), which provides the road map for all PBGC system development and integration, including financial management system integration.

- Implemented interface enhancements for CFS, including the payroll interface modernization, procurement interface, travel interface, and invoice automation. These interfaces provide additional automated capabilities for CFS and reduce the amount of manual data inputs for certain transactions.

  However, major work remains to be completed to provide PBGC with integrated financial management capabilities. PBGC plans to implement the Trust Accounting and FY File System (TAS), which is currently in the design phase. TAS will replace existing financial applications Portfolio Accounting and Management (PAM), FY File, TIS, and TIS Transfer. Additionally, TAS will have automated interfaces with the CMS, CFS, and Integrated Present Value of Future Benefits (IPVFB). TAS implementation is currently planned for August 2012. Additionally, PBGC has identified future capabilities in its financial management to-be architecture including a procurement system a and online budgeting system.

  Recommendation:

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

****

The internal control report recommendations status 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 Gunderson LLP

Calverton, Maryland
November 14, 2011

EXHIBIT I - Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendation Closed During FY 2011:

Recommendation	Date Closed	Original Report Number
FS-10-06	11/2/2011	AUD-2011-3/FA-10-69-2

Prior Year Internal Control Report Recommendation Moved to Management Letter During FY 2011:

Recommendation	Original Report Number
FS-07-06	2008-2/FA-0034-2

Open Recommendations as of September 30, 2011:

Recommendation	Report
Prior Years'	
FS-07-04 *Modified	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 *Modified	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-07-17	2008-2/FA-0034-2
FS-07-16	2008-2/FA-0034-2
FS-07-18	2008-2/FA-0034-2
FS-08-01 *Modified	AUD-2009-2/FA-08-49-2
FS-08-02 *Modified	AUD-2009-2/FA-08-49-2
FS-08-03 *Modified	AUD-2009-2/FA-08-49-2
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 *Modified	AUD-2010-2/FA-09-64-2
FS-09-06 *Modified	AUD-2010-2/FA-09-64-2
FS-09-07	AUD-2010-2/FA-09-64-2
FS-09-08 **[2]	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

EXHIBIT I - Status of Internal Control Report Recommendations

Recommendation	Report
FS-09-16	AUD-2010-2/FA-09-64-2
FS-09-17 *Modified	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
FS-10-01	AUD-2011-3/FA-10-69-2
FS-10-02	AUD-2011-3/FA-10-69-2
FS-10-03 *Modified	AUD-2011-3/FA-10-69-2
FS-10-04	AUD-2011-3/FA-10-69-2
FS-10-05	AUD-2011-3/FA-10-69-2
FY Ended September 30, 2011	
FS-11-01	AUD-2012-1/FA-11-82-1
FS-11-02	AUD-2012-1/FA-11-82-1
FS-11-03	AUD-2012-1/FA-11-82-1
FS-11-04	AUD-2012-1/FA-11-82-1
FS-11-05	AUD-2012-1/FA-11-82-1
FS-11-06	AUD-2012-1/FA-11-82-1
FS-11-07	AUD-2012-1/FA-11-82-1
FS-11-08	AUD-2012-1/FA-11-82-1
FS-11-09	AUD-2012-1/FA-11-82-1
FS-11-10	AUD-2012-1/FA-11-82-1
FS-11-11	AUD-2012-1/FA-11-82-1
FS-11-12	AUD-2012-1/FA-11-82-1
FS-11-13	AUD-2012-1/FA-11-82-1
FS-11-14	AUD-2012-1/FA-11-82-1
FS-11-15	AUD-2012-1/FA-11-82-1
FS-11-16	AUD-2012-1/FA-11-82-1
FS-11-17	AUD-2012-1/FA-11-82-1

[1] *Modified: indicates that the previously reported recommendation has been slightly modified to reflect current conditions.

[2] **Recommendation remains open pending completion by management to acknowledge closure. This recommendation was not included in the FY 2011 financial report.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2011 and 2010 Financial Statements

Audit Report AUD-2012-2 / FA-11-82-2

Section II

Management Comments

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

Office of the Director

MEMORANDUM

November 14, 2011

To: Rebecca Anne Batts
Inspector General

From: Josh Gotbaum
Director

Subject: Response to the Office of Inspector General's (OIG's) Draft Internal Control Report for FY 2011

Thank you for the opportunity to comment on the subject draft report. While there are several issues on which we will need further clarification and discussion as we work together to resolve them, we are in agreement with the vast majority of findings and recommendations and have already taken strides to address them.

We have provided our responses to each recommendation below, and we will be updating our corrective action plans in the near future. As we move forward, we will keep your office informed.

Entity-wide Security Program Planning and Management

1. Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses. **(OIG Control # FS-09-01)**

Response: Management agrees and continues to communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources. This is done in several ways including through an IT Corrective Action Plan (CAP) Executive Steering committee, our Budget committee, recurring investment meetings between OIT and the business areas, and our IT Investment Review Board. A key step in this area is to reinvigorate role based training for Authorizing Officials and Information System Owners this fiscal year.

2. Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 130 identified common security controls. **(OIG Control # FS-08-01 *Modified)**

Response: Management agrees. Following our detailed identification of 130 common controls, all of which are provided via the Agency Security Controls General Support System (ASCGSS), management is now working Plan of Actions and Milestones (POA&Ms) to fix any deficiencies identified in our Security Assessment and Authorization of the General Support Systems.

3. Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control # FS-09-02)**

Response: Management agrees. This will be part of our PBGC POA&M Process which will be implemented in FY 2012.

4. Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies.
(OIG Control # FS-09-03)

Response: Management agrees. Management has already deployed a number of actions to put the foundations of a security program in place during FY 2011. We expect to complete this recommendation in FY 2012.

5. Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control # FS-09-04)**

Response: Management agrees. We have already taken a number of steps to address this recommendation. PBGC has refreshed the Technical Reference Model; established both an Enterprise Target Architecture and a Technology Review Board; and completed a high-level alternatives analysis for infrastructure services. We have also made much progress in refreshing and simplifying hardware and software that is near the end of its service life. Our next actions are to finish the hardware/software refresh and incorporate the alternatives analysis into the infrastructure support contract re-competition. We expect to complete this recommendation in FY 2013.

6. Implement an effective review process to validate the completion of the A&A packages for all major applications. The review should not be performed by an individual associated with the performance of the A&A, or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control # FS-08-02 *Modified)**

Response: Management agrees with this recommendation. We appreciate the auditors' acknowledgement of our progress in this area. We are currently completing an updated information security policy, revised standards, and improved procedures to ensure that the Risk Management Framework, as described in NIST 800-37, Revision 1, is properly implemented at PBGC. A new procedure will address the system registration process by providing the foundation for determining the PBGC Federal Information Security Management Act (FISMA) system inventory, based on boundary and sensitivity impact level. New procedures will address the steps necessary for completing the Security Assessment and Authorization (SA&A) process, including Enterprise Information Security Office (EISO) oversight of the process, consistency in the quality of the SA&A artifacts, and maintenance and storage of these artifacts. The policy, standards, and procedures are scheduled for completion in FY 2012.

7. Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the A&A process for all major applications. **(OIG Control # FS-09-05 *Modified)**

Response: Management agrees. Please see the response to #6, above.

8. Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the A&A review process for major applications. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control # FS-09-06 *Modified)**

Response: Management agrees. Please see the response to #6, above.

9. Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC Office of IT (OIT) operations. **(OIG Control # FS-09-07)**

Response: Management agrees. Please see the response to #6, above.

10. Implement an independent and effective review process to validate the completion of the A&A packages for all major applications. **(OIG Control # FS-08-03A *Modified)**

Response: Management agrees. Please see response to #6, above.

11. Implement an independent and effective review process to validate the completion of the A&A packages for all major applications and general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control # FS-08-03B *Modified)**

Response: Management disagrees with the recommendation as written. However, PBGC does agree that common controls (fully or partially) inherited by applications delivering services to PBGC need to have risk analysis performed that would determine one of the following: (1) the risk that a common control presents is acceptable, (2) testing needs to be performed on the inherited common controls to determine effectiveness with weaknesses identified tracked as POA&M items, or (3) it would be more prudent and cost effective to perform a full (Assessment and Authorization) A&A on the general support systems to ensure PBGC can make an informed decision on whether or not to accept the risk of the application delivering services to PBGC.

12. Develop and implement a process to enforce the dissemination and awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04)**

Response: Management agrees. We are updating the PBGC IT Security Training Program and have already developed both security and privacy awareness training, available to both federal employees and contractor employees on-line. This is part of our development of our zero-day approach to personnel on-boarding. We are also identifying specific roles requiring security training and expect to implement this in FY 2012.

13. Develop and implement an immediate plan of action to address the potential security risk posed by locating the SOC outside of the US. **(OIG Control # FS-10-01)**

Response: Management disagrees, but has an alternative approach to resolving this issue. We have recently been informed by the foreign service provider that Security Operations Center (SOC) is shortly scheduled to be separated from the SOC provider within our borders. In light of this development, we propose obtaining written documents from the latter that provide authoritative and responsible written control descriptions that will assure management regarding the control issues raised.

14. Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and the Federal Information Security Management Act (FISMA). **(OIG Control # FS-10-02)**

Response: Management agrees. Management has taken corrective actions and recently reported this to OIG through our regular reporting process.

15. Ensure that adequate controls in the design and implementation of the SOC are in place to protect PBGC PLUS. **(OIG Control Number # FS-11-XX) 1**

Response: Management disagrees. Please see response to #13, above.

16. Develop controls and implement an ISA and MOU with external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03 *Modified)**

Response: Management agrees. Our agreement is based on the understanding that Interconnection Security Agreements (ISA's) and/or Memoranda of Understanding (MOU's) be executed with systems that interconnect with PBGC, where appropriate. PBGC is managing the related agreements to ensure that they are accurate and updated as needed, and we are maintaining a repository to better track their status. Management has shared information with OIG on the agreements cited in the finding.

Access Controls and Configuration Management

17. Develop and implement procedures and processes for the consistent implementation of common configuration management controls to minimize security weaknesses in general support systems. **(OIG Control # FS-07-07)**

Response: Management is in agreement with this audit recommendation. The recommended corrective actions are expected to be completed in October 2013 as part of the IT Corrective Action Plan.

18. Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control # FS-09-12)**

Response: Management agrees, with our emphasis being on all major systems. Progress on remediating this issue will be made in both FY 2012 and FY 2013.

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

Response: Management is in agreement with this audit recommendation. The recommended corrective actions are expected to be completed in October 2013 as part of the IT Corrective Action Plan.

20. Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control # FS-09-14)**

Response: Management is in agreement with this audit recommendation. The recommended corrective actions are expected to be completed in October 2013 as part of the IT Corrective Action Plan.

21. Ensure test, development and production databases are appropriately segregated to protect sensitive information and fully utilized to increase system performance. **(OIG Control # FS-09-15)**

Response: Management agrees. The recommended corrective actions are expected to make incremental improvements with full resolution in October 2013 as part of the IT Corrective Action Plan.

22. Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control # FS-09-16)**

Response: Management agrees. We will limit the number of developers that have access to production to those responsible for production support and will limit that access to read only functionality to research of production issues in FY 2012.

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

Response: Management agrees. Although this issue and recommendation is focused on the identification and removal of generic accounts, it is related to the overall recertification of accounts issue. PBGC has revised its process and procedures to require the review and recertification of all accounts annually. In FY 2011, this was the basis for the General Support System (GSS) account review. That review included user accounts, as required, and additionally system accounts, generic accounts, and service accounts. The FY 2011 review included the two PBGC GSS's and the 21 major applications. PBGC is formalizing and socializing its recertification process for review and approval by the OIT Governance Board. Future reporting will be completed in FY 2012.

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

Response: Management is in agreement with this audit recommendation. The recommended corrective actions are expected to make incremental improvements with full resolution no later than September 2014 as part of the IT Corrective Action Plan.

25. Assess the risk associated with the lack of segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. **(OIG Control # FS-09-17 *Modified)**

Response: Management agrees. The recommended corrective actions are expected to be completed in FY 2012 as part of the IT Corrective Action Plan.

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

Response: Management agrees. The recommended corrective actions are expected to be completed in FY 2012 as part of the IT Corrective Action Plan.

27. Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed. **(OIG Control # FS-09-18)**

Response: Management agrees. The recommended corrective actions are expected to be completed in FY 2012 as part of the IT Corrective Action Plan.

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

Response: Management agrees. The recommended corrective actions are expected to be completed no later than FY 2014 as part of the IT Corrective Action Plan.

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

Response: Management agrees. We are in the process of implementing automated configuration management monitoring and will begin reviewing several systems' compliance with baseline settings in FY 2012.

30. For the remaining systems, apply controls to lock out and remove inactive and dormant accounts after a specified period in accordance with the IAH.
(OIG Control # FS-07-12 Modified)

Response: Management agrees. The recommended corrective actions are expected to be completed in FY 2012 as part of the IT Corrective Action Plan.

31. Complete the implementation of the recertification process for all user and system accounts. Continue to perform annual recertification and include all PBGC's accounts (e.g. user, generic, service, and systems accounts) for general support systems and major applications.
(OIG Control # FS-07-13)

Response: Management agrees. PBGC initiated an improved process in FY 2011, including email notification to all related Authorizing Officials, Information System Owners, and Information Security Officers from the Senior Agency Information Security Officer, identifying required dates and procedures. We are updating the process and expect completion during the audit review period in FY 2012.

32. Implement controls to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control # FS-07-14)**

Response: Management agrees and is making incremental progress in this area. The recommended corrective actions are expected to be completed no later than FY 2014 as part of the IT Corrective Action Plan.

33. Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control # FS-09-20)**

Response: Management agrees and is making incremental progress in this area. The recommended corrective actions are expected to be completed no later than FY 2014 as part of the IT Corrective Action Plan.

34. Ensure that adequate documentation of access authorization is maintained by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control # FS-07-15)**

Response: Management agrees. PBGC has automated the access authorization process and is in the process of rolling the functionality out. The recommended corrective actions are expected to be completed in FY 2012.

35. 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 # FS-07-16)**

Response: Management agrees. We will be happy to work with you to provide additional evidence that all controls are in alignment with the enforcement of PBGC Directive PM 05-01.

36. Implement a logging and monitoring process for application security-related events and critical system modifications (e.g. CFS, PAS, TAS, PRISM, and IPVFB).
(OIG Control # FS-07-17)

Response: Management agrees. PBGC has identified required controls to address logging and monitoring. We expect completion of work in this area in FY 2013.

37. Replace the Citrix MetaFrame presentation server. **(OIG Control # FS-10-04)**

Response: Management agrees. Management agrees with the recommendation to upgrade the Citrix MetaFrame presentation server, and we are scheduled to do so in FY 2012.

38. Include the application virtualization/application delivery product used by the benefit payments service provider to access the PLUS application in the system boundary. **(OIG Control # FS-10-05)**

Response: Management disagrees. We have performed a risk analysis and have decided to accept the risk.

39. Establish unique accounts for each user in TeamConnect. **(OIG Control # FS-11-XX) 2**

Response: Management agrees. Please see the response to #23, above.

40. Restrict developer's access to production. **(OIG Control # FS-11-XX) 3**

Response: Management agrees. Please see the responses to #26 and #27, above.

41. Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs. **(OIG Control # FS-11-XX) 4**

Response: Management agrees. This will be addressed in the 2012 A&A package.

42. Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control # FS-11-XX) 5**

Response: Management agrees. This will be an interim control, based on the correction of both #39, above, and the shared accounts issue.

Benefits Administration and Payment Department Operations

43. Implement procedures to verify that future contracts for plan asset valuations clearly outline expectations and deliverables in the statement of work. **(OIG Control # FS-11-XX) 6**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

44. Develop a quality assurance program aimed to ensure that plan asset valuations meet the regulatory standard of determining fair market value based on the method that most accurately reflects fair market value. **(OIG Control # FS-11-XX) 7**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

45. Enhance and formalize efforts to improve staff skills, whether Federal or contactor, in planning the valuation reviews, understanding the risks, and developing appropriate scopes and procedures to support credible and reliable results. **(OIG Control # FS-11-XX) 8**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

46. Identify those plans that might potentially have a pervasive misstatement to the financial statements if DOPT asset values were originally misstated. Management should then re-evaluate the DOPT asset values for those identified plans and consider the impact of any known differences on the financial statements. **(OIG Control # FS-11-XX) 9**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

47. Modify the BAPD Operations Manual to explicitly incorporate policies and procedures to archive source records. The BAPD Operations Manual details the process of creating the participant database, but does not explicitly require the archival of source records. Best practice maintenance of source records should include a consolidation of all relevant data in a common location. **(OIG Control # FS-11-XX) 10**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

48. Ensure adequate documentation is maintained which supports, substantiates, and validates benefit payment calculations by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. **(OIG Control # FS-11-XX) 11**

Response: Management agrees. Management will address this recommendation through a corrective action plan.

49. Improve the training of persons tasked with the calculation and review of benefit determinations to ensure their skills are matched with the complexities of the tasks assigned. **(OIG Control # FS-11-XX) 12**

Response: Management agrees. PBGC currently has additional actuarial training scheduled for FY 2012 and will address the issues identified in the finding.

50. Obtain a contract system representative signature on the PLUS MOU or alternatively, develop an interconnection security agreement (ISA) between PBGC and the benefit payments service provider for the connection. **(OIG Control # FS-11-XX) 13**

Response: Management agrees. PBGC will develop an interconnection security agreement (ISA) between PBGC and the service contractor for the connection.

51. Annually review contractor access recertifications for the benefit payments service provider employees with access to PLUS. **(OIG Control # FS-11-XX) 14**

Response: Management agrees. PBGC will annually review contractor access recertifications for the service provider employees with access to PLUS.

52. Review the PLUS contingency plan for compliance with NIST SP 800-34 requirements. **(OIG Control # FS-11-XX) 15**

Response: Management agrees. PBGC will review the PLUS contingency plan for compliance with NIST SP 800-34 requirements.

53. Develop and implement a policy to identify and document the risks associated with PBGC operations performed in foreign countries, ensure appropriate management review, and take appropriate actions to mitigate identified risks. **(OIG Control # FS-11-XX) 16**

Response: We agree. During FY 2012 we will synthesize the various Federal efforts surrounding "cloud" deployment issues for both security and contract issues and incorporate policy in the appropriate places, as needed.

54. For the PLUS SOC operating in a foreign country revise the existing risk assessment to identify and document risks, and take appropriate actions. **(OIG Control # FS-11-XX) 17**

Response: Management disagrees. Please see response to #13, above.

Integrated Financial Management Systems

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

Response: Management agrees. Management appreciates the auditors' acknowledgement of progress made in this complex area. PBGC's planned corrective actions include implementation of the Trust Accounting System (TAS) and the Premium and Practitioner System (PPS). Development of TAS is now under way and scheduled for implementation in FY 2012. Subject to the availability of resources, we anticipate PPS implementation in FY 2014.

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