Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2012 and 2011 Financial Statements Audit

November 15, 2012

AUD-2013-2/FA-12-88-2

This page intentionally left blank.

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

November 15, 2012

To: Josh Gotbuam
Director

Patricia Kelly
Chief Financial Officer

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

Subject: Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2012 and 2011 Financial Statements Audit (AUD-2013-2 / FA-12-88-2)

I am pleased to transmit the attached report prepared by CliftonLarsonAllen LLP resulting from their audit of the PBGC Fiscal Year 2012 and 2011 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, 2012 (AUD-2013-1 / FA-12-88-1). 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 weaknesses.

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

Attachment

This page intentionally left blank.

Report on Internal Controls Related to the Pension Benefit Guaranty Corporation’s Fiscal Year 2012 and 2011 Financial Statements

Audit Report AUD-2013-2 / FA-12-88-2

Contents

Acronyms

ACL	Access Controls List
A&A	Assessment and Authorization
ASD	Actuarial Services Division
ASCGSS	Agency Security Controls General Support System
BAPD	Benefits Administration and Payment Department
CMS	Case Management System
COTS	Commercial-Off-The Shelf
CCRM	Configuration, Change, and Release Management
CI	Configuration Item
CFS	Consolidated Financial System
COOP	Continuity of Operations Program
CCRD	Contracts and Control Review Department
CAP	Corrective Action Plan
DoPT	Date of Plan Termination
EDM	Enterprise Data Model
ELAN	Enterprise Local Area Network
ETA	Enterprise Target Architecture
FIPS PUB	Federal Information Processing Standards Publication
FMFIA	Federal Managers’ Financial Integrity Act of 1982
FY	Fiscal Year
IPS	Image Processing System
IAH	Information Assurance Handbook
IPVFB	Integrated Present Value of Future Benefits
ISA	Interagency Service Agreement

ISO	Information System Owner
IT	Information Technology
MOU	Memorandum of Understanding
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
OPM	Office of Personnel Management
PRISM	Participant Records Information Systems Management
PLUS	Pension and Lump Sum System
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PAM	Portfolio Accounting and Management
PAS	Premium Accounting System
PPS	Premium and Practitioner System
PVFB	Present Value of Future Benefits
RTM	Requirements Traceability Matrix
TAS	Trust Accounting System
TIS	Trust Interface System
TPD	Trusteeship Processing Division

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2012 and 2011 Financial Statements

Audit Report AUD-2013-2 / FA-12-88-2

Section I

Independent Auditor's Report

This page intentionally left blank.

CliftonLarsonAllen

CliftonLarsonAllen LLP
11710 Beltsville Drive, Suite 300
Calverton, MD 20705
301-931-2050 | fax 301-931-1710
www.cliftonlarsonallen.com

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, 2012, 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, 2012 (see Office of Inspector General (OIG) report AUD-2013-1/FA-12-88-1).

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) 2012 financial statements. As reported in our combined report on PBGC's FY 2012 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 43 million workers and retirees in more than 25 thousand private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of the Benefits Administration and Payment Department (BAPD) and information technology (IT). Internal controls over these operations are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

BAPD manages the termination process for defined benefit plans, provides participant services (including calculation and payment of benefits) for PBGC-trusteed plans, provides actuarial support for PBGC, and carries out PBGC's responsibilities under settlement agreements. BAPD has several distinct divisions including Trusteeship Processing Divisions (TPDs) and the Actuarial Services Division (ASD). The TPDs are responsible for capturing the participant data for benefit determinations, managing the benefit payments to participants and beneficiaries, and maintaining the pension plan and participant files that includes underlying documentation used to support the calculation of benefit amounts for the participant and the pension liabilities recorded on PBGC financial statements. The ASD is responsible for calculating the Present Value of Future Benefits (PVFB) liability, based on actuarial assumptions and methods. ASD uses the underlying documentation maintained by the TPDs, as well as mortality tables and interest rate factors, as key inputs to calculate pension plan liabilities recorded on PBGC's financial statements.

BAPD continues to have serious control weaknesses throughout the department. These weaknesses are attributed to BAPD's management and oversight over the processes needed to calculate and value participant's benefits and the related liabilities, as well as to value plan assets. Such weaknesses increase significant risks to PBGC's operations including accurate calculation of plan participants' benefits, accurate financial reporting, and compliance with prescribed laws and regulations. In FY 2012 and 2011, PBGC hired a contractor to perform a review of its programs and activities for improper payments in accordance with the Improper Payment Elimination and Recovery Act. In addition to identifying that actual improper payments occurred, the contractor found that the underlying documentation used to support the benefit payments was not always available. Similar documentation is used to support the actuarial calculations of PBGC pension plan liabilities and related expenses. During FY 2012, we continued to identify numerous deficiencies in BAPD controls that included inadequate documentation to support the calculation of participants' benefits and liabilities, errors in their liability calculations, and errors in valuing plan assets.

The establishment and implementation of the appropriate internal controls are critical to PBGC operations. Furthermore, reliable internal controls ensure that the programs achieve their intended results; resources are used consistent with agency mission, programs and resources are protected from waste, fraud, and mismanagement; laws and regulation are followed; and reliable and timely information is obtained, maintained, reported and used for decision making as stated in the OMB Circular A-123, *Management's Responsibility for Internal Control*. In order to mitigate operational and financial reporting risks to PBGC as a whole, active involvement from BAPD's senior leadership in the monitoring and response to such risks is warranted on a continuous basis.

In response to weaknesses previously identified above, BAPD continues to undergo a strategic review with the intention of addressing the organizational structure and operational issues. In FY 2012, BAPD hired a new Director and continued efforts to develop a plan to address the deficiencies noted in prior OIG financial statements and performance audit reports. PBGC intends the plan to focus on fundamental issues such as internal controls, processes, contractor oversight, training, and staff competencies.

IT continues to be a challenge for management. The safeguarding of PBGC's systems and data is essential to protect PBGC's operations and mission. The OIG and others have consistently identified serious internal control vulnerabilities and systemic security control weaknesses in the IT environment over the last several years. PBGC's delayed progress in mitigating these deficiencies at the root-cause level continued to pose increasing and substantial risks to PBGC's ability to carry out its mission during FY 2012. Due to the persistent nature and extended time required to mitigate such vulnerabilities, additional risks threaten PBGC's ability to safeguard its systems. These risks include technological obsolescence, inability to execute corrective actions, breakdown in communications, and poor monitoring.

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

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

PBGC anticipated completing the assessment and authorization (A&A) process, formerly referred to as a certification and accreditation process, on the Corporation's major applications in FY 2012, but was unable to complete the process. The work on the A&As that has been performed through FY 2012 identified significant fundamental security control weaknesses in PBGC's general support systems, many of which were reported in prior year's audits and remain unresolved. We continued to find deficiencies in the areas of security management, access controls, configuration management, and segregation of duties. Control deficiencies were also found in policy administration, and the completion of A&A for all major applications.

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

The serious weaknesses in BAPD's internal controls such as inadequate documentation to support the benefit and liability calculations, errors in liability calculations and valuing plan assets, as well as the limited progress of mitigating PBGC's systemic security control weaknesses create an environment that could lead to improper application of benefits to plan participations, inaccurate financial reporting and fraud, waste, and abuse.

Based on our findings, we are reporting that the deficiencies in the following areas constitute three material weaknesses for FY 2012:

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

We are also reporting the deficiencies in the following area to be a significant deficiency for FY 2012:

4. Integrated Financial Management Systems

Detailed findings and recommendations follow.

1. Benefits Administration and Payment Department Management and Oversight

BAPD is the core department within PBGC to maintain plan and participant information, and to calculate plan benefits and related liabilities. BAPD's management and oversight function is a key component of the control environment in which its division managers and staff operates. The continuous deficiencies of the aforementioned function increase PBGC's operational and financial reporting risks.

Calculation of the Present Value of Future Benefits Liability

During FY 2012, BAPD made errors in calculating the PVFB liability for some participants. ASD is primarily responsible for the calculation of the PVFB that is recorded on PBGC's financial statements based on actuarial assumptions and methods. These calculation errors were primarily due to two reasons: (1) the actuarial liability factors were applied to incorrect or incomplete data inputs and (2) a plan's particular benefit provisions were not sufficiently reviewed to correctly calculate individual participants' PVFB liability. Specifically, BAPD's ASD used actuarial assumptions because the best available data was not updated into the applicable information system. For example, in some instances an actual date of birth was used to calculate a specific benefit but the estimated date of birth was entered in the applicable information system causing the liability to be incorrect. In other instances, ASD incorrectly calculated certain liabilities of the participants using a single life annuity benefit plan provision instead of the joint and survivorship benefit. During our June 30 interim testing, we identified an error in the calculation of the participant liability for one large plan related to one of the plan's unique provisions. Management was not aware of this unique plan benefit and that it had been inappropriately excluded from the participants' liability calculations. This error required additional efforts by BAPD management to determine the underlying cause and to calculate an overall plan adjustment to PBGC's liability at September 30. Due to these errors noted during the interim period, we adjusted our year-end audit procedures to address the increased operational and financial reporting risks. Using a statistically based sampling technique, we noted approximately 13% of the samples tested in which the liability calculated for a plan participant was either overstated or understated. The projected value of the error to the entire PVFB liability of approximately $106 billion at September 30, 2012, had an estimated range of approximately $507 million understatement to $875 million overstatement and a point estimate of $185 million overstatement.

We also noted deficiencies in BAPD's maintenance of underlying documentation used to support the calculation of the PVFB. BAPD's TPDs are primarily responsible for maintaining the plan and participant files utilized to determine the benefit and liabilities amounts owed to plan participants. The information system that maintains the participant documentation such as birth certificates, marriage certificates, participant benefit applications, plan provisions, salary data, etc., is the Image Processing System (IPS). During our testing at June 30 and September 30, BAPD was not able to provide the documentation needed to support liability calculations for some samples. We also noted that the documentation was not maintained in a single systematic manner and required herculean efforts by BAPD and other PBGC departments to locate and provide the documentation. The lack of appropriate documentation results in limited physical and financial controls, and could lead to improper benefit payment and participant liability calculations by PBGC. Consequently, we could not determine whether the benefits or the associated liability was calculated properly for those selected samples at June 30 and September 30.

Last year we reported several deficiencies in BAPD related to documentation, including the need to require archival of source documents, implementation of controls to ensure monitoring and enforcement of procedures requiring document maintenance, and to improve the training of persons tasked with calculating and reviewing benefit determinations. These deficiencies have not yet been corrected.

Because of errors in the liability calculations and the lack of supporting documentation, PBGC is at risk for inaccurately valuing the plan liabilities reported in its financial statements. Also, these deficiencies could impact PBGC management's ability to provide meaningful and accurate information to its key stakeholders such as the plan participants, the Board, Congress, and OMB.

Recommendations:

- PBGC should promptly correct the errors in its calculations identified by the auditors. **(OIG Control Number # FS-12-01)**

- PBGC should develop and implement a comprehensive documentation retrieval system that clearly identifies the location of the participants' census data and benefit calculation elements in a systematic manner. **(OIG Control Number # FS-12-02)**

- PBGC should update the technical reference guide used by ASD to document the procedures used to calculate the qualified pre-survivor annuity and deferred retirement ages. **(OIG Control Number # FS-12-03)**

- Update current procedures to ensure that all plan provisions are considered in the calculation of the individual participant liability. The procedures should be documented in a formal procedural manual and/or checklist. **(OIG Control Number # FS-12-04)**

- PBGC should refine their current procedures for processing plans and uploading participant data in the Genesis database to ensure that the best available data is used to support benefit payments and Integrated Present Value liabilities. **(OIG Control Number # FS-12-05)**

- 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) (PBGC scheduled completion date: June 30, 2014)**

- Ensure that 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) (PBGC scheduled completion date: June 30, 2012)**

- 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-11-12) (PBGC scheduled completion date: December 31, 2012)**

Valuation of Plan Assets and Benefits

Although BAPD has undertaken efforts to revalue assets for certain pension plans trusteed by PBGC, internal control weaknesses in this area continue to merit focus. The fair market value of a pension plan's assets at the date of plan termination (DoPT) is an essential factor needed to determine the retirement benefit amounts owed to plan participants. The lack of BAPD's effective oversight and monitoring of contracted reviews over asset valuations continued to pose significant risks to the participants' benefit determinations. During FY 2012, BAPD hired contractors to perform revaluations of plan assets for some large plans which resulted in increased benefits owed to certain plan participants. BAPD management stated that a risk analysis is currently underway to determine which additional pension plans may have asset valuation misstatements and pose the greatest risks to the participants' benefit payments. This risk analysis was not complete at September 30, 2012. In addition, management has yet to finalize a quality control review process to verify and validate the satisfactory completion of contracted DoPT plan asset valuation audits, and to establish a detailed process to ensure the consistent application of a methodology to determine the fair market value of plan assets at DoPT at September 30, 2012.

Additional weaknesses identified as part of the prior year financial statement audit stemmed from inadequate management of contractors, a condition that continues to exist. As previously discussed, these contractors perform critical functions such as the valuing of plan assets. Services provided by contractors should be subject to an effective system of internal controls. Management has not always fully considered the exposure and risk that contractors introduce into its environment. BAPD intended to develop corrective action plans in FY 2012 to focus on fundamental issues such as internal controls, processes, contractor oversight, and training and staff competencies. However, the development of these plans was still in progress at September 30, 2012.

Recommendations:

- Continue to 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) (PBGC scheduled completion date: April 30, 2013)**

- Continue to 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) (PBC scheduled completed date: April 30, 2013)**

- Continue to 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) (PBC scheduled completed date: April 30, 2013)**

- 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) (PBC scheduled completed date: December 30, 2012)**

2. Entity-wide Security Program Planning and Management

In prior years, we reported that PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. Deficiencies persisted in FY 2012, which 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.

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 a continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

In the *Federal Information Security Management Act of 2002*, Congress required 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.

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. However, PBGC continued to improve the PBGC Enterprise Information Security Program which includes strengthening the system authorization process, verifying contractor A&A deliverables, and ensuring their quality and conformance to the statement of work as well as to the objectives of the PBGC risk management process and NIST SP 800-53. PBGC has focused on updating the underlying policies, strengthening the security program overall, obtaining quality contractors to conduct the assessments, and ensuring PBGC prepare for and begin the execution of the system authorization process.

- NIST 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 their corrective actions in early 2015, as of the end of FY 2012, 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. PBGC realizes these challenges, and has identified and documented the enterprise common security controls in the Agency Security Controls General Support System (ASCGSS) System Security Plan. PBGC completed and approved the Infrastructure Configuration Management Plan in FY 2012. The Corporation also approved its CCRM process and procedures in FY 2012. The future implementation of these strategies is designed to enable PBGC to implement a disciplined and integrated approach to CCRM, eliminate inconsistencies and weaknesses in the implementation of the processes and procedures and ensure compliance with the NIST SP 800-53, Rev 3 common controls. However PBGC had not completed and confirmed the implementation, and operating effectiveness of its common security controls; management cannot have confidence that the controls were implemented.

  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) (PBGC scheduled completion date: June 30, 2013)**

  - Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 130 identified common security controls. **(OIG Control # FS-08-01) (PBGC scheduled completion date: February 28, 2015)**

  - Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented. **(OIG Control # FS-09-02) (PBGC scheduled completion date: September 30, 2012)**

  - 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) (PBGC scheduled completion date: September 30, 2012)**

  - Complete the development and implementation of the redesign of PBGC's IT infrastructure; and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls. **(OIG Control # FS-09-04) (PBGC scheduled completion date: February 28, 2015)**

  - Implement an effective review process to validate the completion of the A&A packages for all major applications. The review should not be performed by an individual associated with the performance of the A&A, or by someone who could influence the results. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained. **(OIG Control # FS-08-02) (PBGC scheduled completion date: June 30, 2013)**

  - Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the A&A process for all major applications. **(OIG Control # FS-09-05) (PBGC scheduled completion date: September 30, 2012)**

  - Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the A&A review process for major applications. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress. **(OIG Control # FS-09-06) (PBGC scheduled completion date: September 30, 2012)**

  - Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC OIT operations. **(OIG Control # FS-09-07) (PBGC scheduled completion date: September 30, 2012)**

  - Implement an independent and effective review process to validate the completion of the A&A packages for all major applications. **(OIG Control # FS-08-03) (PBGC scheduled completion date: June 30, 2013)**

  - Implement a documented, independent and effective review process to validate the completion of the A&A packages for general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments. **(OIG Control # FS-08-03) (PBGC scheduled completion date: September 30, 2012)**

- Information security policies and procedures were not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for all needed security awareness training. PBGC published SE-PRC-01-01, *Security Awareness and Training Procedures*, in June 2012. It defines both annual security awareness requirements and role-based requirements. Security incident response training is still in development and will be delivered during FY 2013 for all staff involved in security incident management and response. PBGC is in its second year of providing an online information security awareness module supplied by an OMB-approved Information System Security Line of Business provider (OPM's Go Learn Learning Management System platform). This enables more efficient tracking of staff and contractors who have taken the module. PBGC fulfilled last year's requirement for general security awareness training using this service. Role-based training for security is still in the development stage. Lack of security awareness can lead to increased risk of security breaches and exposure to fraud. Controls may not be placed in operation as mandated by PBGC policies.

Recommendation:

- o Continue to disseminate the awareness of PBGC's security policies and procedures through adequate training. **(OIG Control # FS-07-04) (PBGC scheduled completion date: September 30, 2012)**

- PBGC has not executed ISAs or MOUs 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 ISAs with all external organizations' systems. In the absence of an ISA and MOU, either party (PBGC or external system owner) may be unfamiliar with the technical requirements of the interconnection and the details that may be required to provide overall security for systems that are interconnected.

  Recommendation:

  - o Develop controls and implement an ISA or MOU with all external organizations whose systems connect to PBGC's systems. **(OIG Control # FS-10-03) (PBGC scheduled completion date: September 30, 2012)**

3. 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. PBGC realizes these challenges, and is implementing a disciplined and integrated approach through development of *Configuration, Change, and Release Management (CCRM) Process & Procedures* consistent with NIST SP 800-53, Rev 3. The Corporation has also developed and is implementing additional policies and procedures, including deploying technical and configuration management tools. Technical tools have been or are being deployed to better manage configuration of common operating platforms. Once these tools are fully operational in the infrastructure, they will help ensure that controls related to the configuration of infrastructure components remain consistent and provide alerting capabilities when components are changed. Other complementary processes, such as the Tiger Team focus on system scanning and vulnerability management, support PBGC's capability to carefully document and validate system vulnerabilities and also provide evidence as to the operating effectiveness of some technical common controls.

Access controls should be in place to consistently limit and 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 2012 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 inconsistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server configurations; therefore, management cannot rely on results obtained in the development or test environments prior to deployment in production. Overall, the PBGC environment suffers from inadequate configuration, roles, privileges, logging, monitoring, file permissions, and operating system access.

- 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 2012, 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.
  - Back out plans for reversing system changes, in case of an unexpected situation, are not consistently documented.

    PBGC recognized that the agency lacked a mechanism for controlling the flow of data between the development, test and production environments. PBGC plans to implement firewalls with associated policies and business rules to control the information flows between environments. The Corporation developed a high-level conceptual design for segregating the environments, the solution was accepted and procurement was issued for hardware and services that will segregate the environments

    In the interim, PBGC implemented the Access Control Lists (ACLs) that will act as static firewalls until the comprehensive solution is fully implemented. The ACLs are intended to control the flow of data between environments and stop any new flows from starting unless there is an approved change request.

- PBGC has made improvement in developing baseline configuration management controls. PBGC began implementing its CCRM process, procedures and diagrams in FY 2012, establishing the guidance for how Configuration Items (CIs) are identified and baselines established, how CI changes are controlled (Change Management) and managed through environments (Release Management), and how CIs and baselines are verified and audited using status accounting. The Change Management processes, procedures and diagrams provide the governance structure as to which CI changes are authorized to be promoted through various environments. The Corporation is in the process of deploying and/or procuring automated tools to facilitate the execution of Configuration Management activities with a specific emphasis in applying controls to authentication parameters to PBGC General Support Systems and allowing for the manual review of noted deviations from baseline settings. The tools will provide the capability to establish a baseline of CIs that exist at PBGC and also the ability to monitor compliance with the configuration management controls in an automated manner.

- 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) (PBGC scheduled completion date: October 31, 2013)**

- Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control # FS-09-12) (PBGC scheduled completion date: October 31, 2013)**

- Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # FS-09-13) (PBGC scheduled completion date: October 31, 2013)**

- Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards. **(OIG Control # FS-09-14) (PBGC scheduled completion date: October 31, 2013)**

- Ensure test, development and production databases are appropriately segregated to protect sensitive information, and fully utilized to increase system performance. **(OIG Control # FS-09-15) (PBGC scheduled completion date: October 31, 2013)**

- Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented. **(OIG Control # FS-09-16) (PBGC scheduled completion date: October 31, 2013)**

- PBGC's policies and practices have not effectively restricted the addition of unnecessary and generic accounts to systems in production. Consequently, the number of unnecessary and generic accounts grew over the years. Furthermore, PBGC's configuration management weaknesses have contributed significantly to its inability to effectively implement controls to ensure the consistent removal and locking out of generic or dormant accounts. PBGC has made progress in the recertification and dormant Account Process. However, not all major systems have gone through the recertification process such as those in the Benefits Administration and Payment Department. Furthermore, the actual removal of dormant accounts from systems is still a manual process and remains a risk to the timeliness of effective removal. The lack of controls to remove/disable inactive accounts and dormant accounts exposes PBGC's systems to exploitation and compromise. PBGC has taken action to review generic accounts in the general support system, removing those that are unnecessary, and approving those that are necessary; however, more work is needed to ensure that all unnecessary and generic accounts are removed. Failure to identify and remove unnecessary accounts from the system could result in PBGC's systems being at an increased risk for unauthorized access, modification, or deletion of sensitive system and/or participant information.

Recommendations:

- Continue to remove unnecessary user and generic accounts. **(OIG Control # FS-07-08) (PBGC scheduled completion date: July 31, 2012)**

- Assess the risk associated with the lack of segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance. **(OIG Control # FS-09-17) (PBGC scheduled completion date: February 15, 2013)**

- For the remaining systems, apply controls to remove/disable inactive and dormant accounts after a specified period in accordance with the IAH. **(OIG Control # FS-07-12) (PBGC scheduled completion date: July 31, 2012)**

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

  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 codes into the production environment.

  Recommendation:

  - Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10) (PBGC scheduled completion date: December 31, 2012)**

- 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:

- Consistently apply controls to ensure that authentication parameters for PBGC's general support systems (e.g. Novell, Windows, Sun Solaris, Oracle, etc.) and applications comply with the IAH. **(OIG Control # FS-07-11) (PBGC scheduled completion date: July 31, 2014)**

- Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings. **(OIG Control # FS-09-19) (PBGC scheduled completion date: October 31, 2013)**

- The OIT recertification process remains incomplete and does not include all user and system accounts. In addition, the Recertification of User Access Process, version 4.0, does not explicitly state that all accounts (e.g. user, system, and service) across all platforms and applications will be recertified annually. PBGC's infrastructure design and configuration management weaknesses have contributed significantly to its inability to effectively implement controls to recertify all user and system accounts. The recertification process is still undergoing changes to ensure all major information systems are reviewed. PBGC implemented an automated eLAN workflow process at the end of FY 2011, which provided another way for PBGC's customers to interact with the Service Desk and submit network and application services (eLAN) access requests. Effective May 1, 2012, PBGC required that users discontinue submitting paper eLAN forms and instead use the automated system, except in situations where the automated system does not accommodate a user's unique and specific access request due to services and functions that aren't available in PBGC's current Service Catalog. In those cases, the Service Desk is prepared to assist the user with the completion of the paper eLAN until the automated system can be modified. Current plans are to incorporate additional workflow modifications, to eliminate the need for any paper forms, into a planned Service Manager, version 7 to version 9 migration which is scheduled for FY 2013.

  Unauthorized users could gain access to PBGC's data and personally identifiable information. 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 # FS-07-13) (PBGC scheduled completion date: July 31, 2013)**

- Vulnerabilities found in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. These PBGC system vulnerabilities are caused by an ineffective deployment strategy in the development, test, and production environments. Ineffective system deployments have resulted in an environment that is in disarray. PBGC has deployed additional technical tools to address this weakness, but requires additional cycle time to determine effectiveness.

Security control weaknesses and vulnerabilities in key databases remain unresolved. These control weaknesses are scheduled to be corrected in 2013. These weaknesses expose PBGC to increased risk of data modification or deletion. Unauthorized changes could occur and not be detected.

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 # FS-07-14) (PBGC scheduled completion date: October 31, 2013)**

- Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments. **(OIG Control # FS-09-20) (PBGC scheduled completion date: October 1, 2014)**

- 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) (PBGC scheduled completion date: April 30, 2013)**

- The application virtualization/application delivery product used by PBGC's benefit payments service provider to connect to its benefit payments system, PLUS, is not included in the system boundary when conducting the A&A for the PLUS application. There is no documented security plan, risk assessment, security controls testing and continuous monitoring program for the application virtualization/application delivery product.

- 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:

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

- Establish unique accounts for each user in TeamConnect. **(OIG Control # FS-11-02) (PBGC scheduled completion date: TBD)**

- Restrict developer's access to production. **(OIG Control # FS-11-03) (PBGC scheduled completion date: September 30, 2012)**

- Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs. **(OIG Control # FS-11-04) (PBGC scheduled completion date: TBD)**

- Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control # FS-11-05) (PBGC scheduled completion date: TBD)**

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, *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, government-wide, 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:

Lack of standard data classifications and common data elements:

- 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 the use of 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 multiemployer 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 in FY 2012 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) in January 2013, after completing the TAS user acceptance testing. The design of TAS is based on an externally-hosted, commercial-off-the-shelf investment accounting package. TAS is another step closer to financial management systems integration, as it replaces Portfolio Accounting and Management (PAM), TIS, and FY File. TAS will replace the following existing financial applications: PAM, FY File, Trust Interface System (TIS), and TIS Transfer. Additionally, TAS will have automated interfaces with the CMS, CFS, and IPVFB. Lastly, PBGC has identified future capabilities in its financial management to-be architecture including a procurement system and an online budgeting system.

PBGC's IT initiatives include further corrective actions through the implementation of TAS and the Premium and Practitioner System (PPS). Also during FY 2012, PBGC began the development of PPS. PPS will be fully integrated with the Oracle eBusiness Suite COTS solution used for PBGC's Consolidated Financial Systems, and will replace the PAS in December 2013.

Recommendation:

- o PBGC needs to implement and execute a plan to integrate its financial management systems in accordance with OMB Circular A-127. **(OIG Control # FS-07-18) (PBGC scheduled completion date: September 30, 2013)**

****

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.

CliftonLarsonAllen LLP

Calverton, Maryland
November 14, 2012

EXHIBIT I - Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendation Closed For FY 2012:

Recommendation	Date Closed	Original Report Number
FS-07-09	11/13/2012	2008-2/FA-0034-2
FS-07-15	11/13/2012	2008-2/FA-0034-2
FS-07-16	11/13/2012	2008-2/FA-0034-2
FS-09-08	11/13/2012	AUD-2010-2/FA-09-64-2
FS-09-10	11/13/2012	AUD-2010-2/FA-09-64-2
FS-09-18	11/13/2012	AUD-2010-2/FA-09-64-2
FS-10-01	11/13/2012	AUD-2011-3/FA-10-69-2
FS-10-02	11/13/2012	AUD-2011-3/FA-10-69-2
FS-10-04	11/13/2012	AUD-2011-3/FA-10-69-2
FS-11-01	11/13/2012	AUD-2012-2/FA-11-82-2
FS-11-13	11/13/2012	AUD-2012-2/FA-11-82-2
FS-11-14	11/13/2012	AUD-2012-2/FA-11-82-2
FS-11-15	11/13/2012	AUD-2012-2/FA-11-82-2
FS-11-17	11/13/2012	AUD-2012-2/FA-11-82-2

Prior Year Internal Control Report Recommendation Moved to Management Letter During FY 2012:

Recommendation	Original Report Number
FS-11-16	AUD-2012-2/FA-11-82-2

Open Recommendations as of September 30, 2012:

Recommendation	Report
Prior Years'	
FS-07-04	2008-2/FA-0034-2
FS-07-07	2008-2/FA-0034-2
FS-07-08	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-07-17	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
FS-08-03	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

Recommendation	Report
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-09-09 [1]	AUD-2010-2/FA-09-64-2
FS-09-11 [1]	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-09-19	AUD-2010-2/FA-09-64-2
FS-09-20	AUD-2010-2/FA-09-64-2
FS-10-03	AUD-2011-3/FA-10-69-2
FS-10-05	AUD-2011-3/FA-10-69-2
FS-11-02	AUD-2012-2/FA-11-82-2
FS-11-03	AUD-2012-2/FA-11-82-2
FS-11-04	AUD-2012-2/FA-11-82-2
FS-11-05	AUD-2012-2/FA-11-82-2
FS-11-06	AUD-2012-2/FA-11-82-2
FS-11-07	AUD-2012-2/FA-11-82-2
FS-11-08	AUD-2012-2/FA-11-82-2
FS-11-09	AUD-2012-2/FA-11-82-2
FS-11-10	AUD-2012-2/FA-11-82-2
FS-11-11	AUD-2012-2/FA-11-82-2
FS-11-12	AUD-2012-2/FA-11-82-2
FY Ended September 30, 2012	
FS-12-01	AUD-2013-2/FA-12-88-2
FS-12-02	AUD-2013-2/FA-12-88-2
FS-12-03	AUD-2013-2/FA-12-88-2
FS-12-04	AUD-2013-2/FA-12-88-2
FS-12-05	AUD-2013-2/FA-12-88-2

[1] Recommendation remains open pending completion by management to acknowledge closure. This recommendation was not included in the FY 2012 financial report.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2012 and 2011 Financial Statements

Audit Report AUD-2013-2 / FA-12-88-2

Section II

Management Comments

This page intentionally left blank.

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, 2012

To: Rebecca Anne Batts
Inspector General

From: Josh Gotbaum Josh Gotbaum
Director

Subject: Response to the Draft FY 2012 Internal Control Report

Thank you for the opportunity to comment on the subject draft report. We are in agreement with the reports' five new recommendations identified for FY 2012, and have provided details regarding our corrective actions and estimated completion dates in the attachment to this memorandum. We are already making progress in implementing them.

Regarding agreed-upon recommendations from prior years, we continue to enhance our controls relating to our IT security program, strengthening access controls and configuration management, enhancing system integration efforts, and improving our pension administration practices. In particular, during FY2012, PBGC established a Tiger Team to urgently address critical and high vulnerability risks identified in OIG's FY2011 Penetration Test. Results were reviewed with OIG, and PBGC has incorporated cyclical scanning and patching vulnerabilities as a part of current operations.

As work on these recommendations is completed, we will continue to provide your office with evidence regarding the corrective actions taken. Also, we look forward to resolution of other prior year recommendations which are the subject of ongoing discussions with your office.

Attachment

cc:

Laricke Blanchard
Patricia Kelly
Alice Maroni
Ann Orr
Michael Rae
Srividhya Shyamsunder
Judith Starr
Martin O. Boehm
Philip Langham
Theodore J. Winter

Attachment

1. **OIG Recommendation:** PBGC should promptly correct the errors in its calculations identified by the auditors.

   PBGC Response:

   BAPD concurs. BAPD will analyze the calculation errors once received from the independent audit and will develop an action plan to identify and take corrective action as appropriate.

   Targeted completion date: 06/2013

2. **OIG Recommendation:** PBGC should develop and implement a comprehensive documentation retrieval system that clearly identifies the location of the participants' census data and benefit calculation elements in a systematic manner.

   PBGC Response:

   BAPD concurs. BAPD will refocus our efforts to ensure that we collect and audit data and clearly establish procedures that outlines where participant data is stored. In addition, data management is one area of focus in the BAPD Strategic Review and will be improved over the short and long term through fiscal year 2018.

   Targeted completion date: 6/2013

3. **OIG Recommendation:** PBGC should update the technical reference guide used by ASD to document the procedures used to calculate the qualified pre-survivor annuity and deferred retirement ages.

   PBGC Response:

   BAPD concurs. ASD will update the technical reference guide to include the procedures used to calculate the qualified pre-survivor annuity and deferred retirement ages.

   Targeted completion date: 6/2013

4. **OIG Recommendation:** PBGC should update current procedures to ensure that all plan provisions are considered in the calculation of the individual participant liability. The procedures should be documented in a formal procedural manual and/or checklist.

   PBGC Response:

   BAPD concurs. BAPD revised the TPD Software Review Checklist to clarify the identification of plan provisions that affect the IPV. ASD will review the IPVFB supplemental tables and make corrections specifically identified in our review of non-level benefits. The actuaries will be provided additional training to re-enforce how unusual forms of benefits and other plan provisions should be stored in the valuation database and reported to ASD/IPVFB and OASD.

   Targeted completion date: 3/2013

5. **OIG Recommendation:** PBGC should refine their current procedures for processing plans and uploading participant data in the Genesis database to ensure that the best available data is used to support benefit payments and Integrated Present Value liabilities.

   PBGC Response:

   BAPD concurs. BAPD will review current applicable procedures for processing plans and uploading data into the Genesis database to ensure that the best available data is used to support benefit payments and IPV liabilities.

   Targeted completion Date: 6/2013

This page intentionally left blank.

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