Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2013 and 2012 Financial Statements Audit

November 15, 2013

AUD 2014-3/FA-13-93-2

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, 2013

To: Josh Gotbaum
Director

Patricia Kelly
Chief Financial Officer

From: Rashmi Bartlett
Assistant Inspector General for Audit

Subject: Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Years 2013 and 2012 Financial Statement Audit (AUD-2014-3/FA-13-93-2)

I am pleased to transmit the report prepared by CliftonLarsonAllen LLP resulting from their audit of the PBGC Fiscal Year 2013 and 2012 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 15, 2013 (AUD-2014-2 / FA-13-93-1).

Management's response to this report is attached in full and 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 note that the seven recommendations are unresolved because PBGC management has not established completion dates for the recommendations. Within 30 days please provide me with a corrective action plan and an estimated completion date for each unresolved recommendation.

Over the course of years, the Office of Inspector General has developed an effective and professional working relationship with the Corporation that enables us to accomplish the audit timely. We appreciation the overall cooperation provided during the performance of this year's audit.

Attachment

cc: Alice Maroni
Joni Palmer
Ann Orr
Sanford Rich
Barry West
Judith Starr
Ted Winter
Marty Boehm

This page intentionally left blank.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2013 and 2012 Financial Statements

Audit Report AUD-2014-3 / FA-13-93-2

Contents

Section I: Independent Auditor's Report

Section II: Management Comments

This page intentionally left blank.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2013 and 2012 Financial Statements

Audit Report AUD-2014-3 / FA-13-93-2

Acronyms

AED	Asset Evaluation Division
ASD	Actuarial Services Division
BAPD	Benefits and Payment Department
CCRM	Configuration, Change and Release Management
CFS	Consolidated Financial System
CRM	Customer Relationship Management
CSAM	Cyber Security Assessment and Management
EMC	Executive Management Committee
FIPS	Federal Information Processing Standards
FY	Fiscal Year
IT	Information Technology
IPVFB	Integrated Present Value of Future Benefits
NIST	National Institute of Standards and Technology
NIST SP	National Institute of Standards and Technology Special Publication
OMB	Office of Management and Budget
OIG	Office of Inspector General
PAS	Premium Accounting System
PBGC	Pension Benefit Guaranty Corporation
PPS	Premium and Practitioner System
POAM	Plan of Action and Milestones
PRAD	Policy, Research and Analysis Department
PRISM	Participant Records Information System Management
PVFB	Present Value of Future Benefits
PVMG	Patch and Vulnerability Management Group
SA&A	Security Assessment and Authorization
TAS	Trust Accounting System
TPD	Trust Processing Division

This page intentionally left blank.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2013 and 2012 Financial Statements

Audit Report AUD-2014-3 / FA-13-93-2

Section I

Independent Auditor's Report

This page intentionally left blank.

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Pension Benefit Guaranty Corporation

To the Board of Directors, Management,
and Acting 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, 2013, 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 15, 2013 (see Office of Inspector General (OIG) report AUD 2014-2/FA-13-93-1).

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) Bulletin No. 14-02, *Audit Requirements for Federal Financial Statements*.

In our combined report on PBGC's FY 2013 financial statements, we identified certain deficiencies in internal control that we consider material weaknesses, and another deficiency that we consider to be a significant deficiency. The purpose of this report is to provide more detailed discussions of the specifics underlying the deficiencies reported in the internal control section of our combined report on PBGC's fiscal year (FY) 2013 financial statements.

Summary

PBGC protects the pensions of approximately 42 million workers and retirees in nearly 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.

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 regulations 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 PBGC's senior leadership in the monitoring and response to such risks is warranted on a continuous basis.

Based on our findings, we are reporting that the deficiencies in the following areas constitute three material weaknesses for FY 2013:

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 2013:

4. Integrated Financial Management Systems

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.

1. Benefits Administration and Payment Department Management and Oversight

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), the Actuarial Services Division (ASD) and the newly formed Asset Evaluation Division (AED). 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 AED will be responsible for ensuring that the plan asset valuations meet the regulatory requirements standard for determining the fair market value of assets. 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 has implemented corrective actions to address the control weaknesses. These corrective actions consisted of modifying the BAPD operations manual, issuing a records management manual, developing staff training materials and updating technical reference guides, Furthermore, the BAPD Director restructured the department divisions and created the AED to better align staff core competencies and skills with the intent to mitigate operational and financial reporting risks.

Even with these corrective actions, BAPD continues to have 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 pose significant risks to PBGC's operations including inaccurate calculation of plan participants' benefits, inaccurate financial reporting, and noncompliance with prescribed laws and regulations. During FY 2013, we continued to identify deficiencies in BAPD controls that included errors in their liability calculations, inadequate documentation to support the calculation of participants' benefits and liabilities, and errors in valuing plan assets.

Calculation of the Present Value of Future Benefits Liability

We continued to identify errors in the calculation of participant benefits and the related PVFB liability. During our testing of the PVFB liability reported at June 30 and September 30, we noted:

- errors in valuing participant benefits and associated liability that were caused by system capability limitations or programming flaws;
- archival procedures for documentation maintenance in place at the time of certain plan terminations were not adequate; and
- data entry errors and inaccurate use of plan data.

These long standing deficiencies in BAPD processes continue to impede management's ability to accurately calculate valuations for some participant's benefits and related future liabilities. Using a statistically based sampling technique, we noted approximately 20% 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 $105 billion at September 30, 2013, had an estimated range of approximately $728 million understatement to $414 million overstatement and a point estimate of $157 million overstatement.

In addition, BAPD's maintenance of underlying documentation used to support the calculation of the PVFB continued to be a significant challenge. The information system that maintains the participant documentation needed to calculate benefits such as birth certificates, marriage certificates, participant benefit applications, plan provisions and salary data is the Image Viewer System. 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. 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. As a result, 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 fully 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-13-01)**

- PBGC should develop and implement improvements to the BAPD Systems (Spectrum and the Integrated Present Value of Future Benefits (IPVFB)) systems to:
  - Record and value separate benefit components payable under different annuity forms
  - Record and value anticipated future benefit amount changes
  - Value temporary joint and survivorship (J&S) benefits **(OIG Control Number # FS-13-02)**

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

- PBGC should continue to 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 IPVFB liabilities **(OIG Control # 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 # 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; revised date: June 30, 2014)**

- Improve the training for all levels of staff 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 MODIFIED) (PBGC scheduled completion date: December 31, 2012; revised date: TBD)**[**]

Valuation of Plan Assets and Benefits

BAPD has undertaken significant efforts to revalue assets for certain pension plans trusteed by PBGC. These efforts have yet to be fully implemented and the internal control weaknesses continue to merit focus.

The fair market value of a pension plan's assets at the date a plan is terminated is an essential factor needed to determine the retirement benefit amounts owed to plan participants. BAPD's ineffective

[*] PBGC has not established a revised completion date.

[**] PBGC submitted documentation to close this recommendation. The auditors determined that further management clarification or corrective action was needed. PBGC needs to provide a revised completion date based on the OIG's feedback.

oversight of contracted reviews over asset valuations in the past continued to pose significant risks to the participants' benefit determinations. In FY 2013, BAPD hired a contractor to develop new plan asset valuation procedures for the newly formed AED. As a test, these procedures were used by the contractor to value the assets of only two terminated plans. The contractor evaluated the operating effectiveness of its procedures and provided its assessment to BAPD management.

Currently, BAPD management has yet to conduct an independent evaluation of the contractor's procedures to determine their sufficiency and adequacy on valuing pension plan assets. Furthermore, BAPD did not complete the re-work of certain plan asset valuations based on its risk based approach to determine whether participant's benefits require any adjustment. The plan asset valuations are expected to be completed in FY 2014.

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 # FS-11-06) (PBGC scheduled completion date: April 30, 2013; revised date: December 31, 2013)**

- Continue to develop and assess the effectiveness of 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-11-07) (PBGC scheduled completed date: April 30, 2013; revised date: TBD)****

- Continue to identify those plans that might potentially have a pervasive misstatement to the financial statements if date of plan termination (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-11-09) (PBC scheduled completed date: December 31, 2012; revised date: December 31, 2013)**

IT Material Weaknesses

PBGC has made progress in addressing IT security weaknesses at the root-cause level by establishing the foundation for effective security controls within the National Institutes of Standards and Technology (NIST) Risk Management Framework, but these controls require time to mature and show evidence of their effectiveness. PBGC has continued to lay the groundwork in the deployment of tools, acquisition of staff, and development of approaches that will enable the PBGC to better manage the design, implementation, and operational status and effectiveness of its IT security controls. PBGC has continued to develop and implement procedures and processes for the consistent implementation of common security and configuration management controls to minimize security weaknesses.

Communication of information security progress and deficiencies to the PBGC Executive Management Committee (EMC) has improved, with briefings in February and June 2013 as part of a new process to hold PBGC more accountable to audit deadlines and inform senior management of issues, barriers, and priorities to address closure of audit findings.

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. Though progress was made as highlighted below, deficiencies persisted in FY 2013, which prevented PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. An entity-wide information security management program is the foundation of a security control structure and is 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.

PBGC has now established the foundation for implementing a more effective entity-wide security program. In 2013, PBGC issued the *IT Security Architectural Analysis Recommendations Report* that provides a blueprint for implementing entity-wide controls and addressing PBGC's security program's strengths, weaknesses, threats, and opportunities. PBGC also completed work on a long-standing weakness relating to Interconnection Security Agreements with all external organizations whose systems connect with PBGC systems.

PBGC acquired services from the Department of Justice to use their hosted Cyber Security Assessment and Management (CSAM) system to automate and support a consistent and effective approach to Plan of Action and Milestones (POA&M) management, the development and maintenance of security artifacts, and the management of common controls. Migration of POA&Ms and artifacts is underway.

While the *IT Security Architectural Analysis Report* represents progress, much remains to be done to implement and ensure adequate operation of controls. PBGC is still in the process of implementing a continuous monitoring program through the deployment and implementation of automated and manual tools, processes and procedures. 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 are as follows:

- <u>Security Assessments and Authorizations (SA&As) for several major applications not completed</u>. SA&A serves as a control to verify and validate that system security controls are properly implemented and working correctly. While a majority of SA&As have been completed by the Bureau of Public Debt through an interagency agreement with PBGC, this long standing issue is critical to complete. PBGC reported that, as a result of an updated inventory registration process, it identified several additional systems that require SA&As. The new *Office of Information Technology*

Enterprise Information Security Authorization & Assessment Package Review Work Instructions, dated August 27, 2013, and the migration to CSAM will assist PBGC in completing the SA&A for its major applications.

- Less than one-half of security controls implemented. Using NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, PBGC identified 208[1] common security controls PBGC stated that 93 of these controls have been implemented. While PBGC anticipates completion of their corrective actions in early 2015, as of the end of FY 2013, they have not documented the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of the remaining 115 identified common security controls. This places PBGC at risk for insufficient protection of sensitive or critical resources or disproportionately high expenditures for common security controls. Without full development and implementation, common security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied.

- Security infrastructure design and implementation weaknesses continue. PBGC's ability to effectively implement common security controls across its systems and applications was adversely affected because there are weaknesses in its infrastructure design and deployment strategy for systems and applications. Historic weaknesses in PBGC's infrastructure design and deployment strategy for systems and applications continued to adversely affect its ability to effectively implement common security controls across its systems and applications. Such conditions lead to inadeqate protection of sensitive or critical resources or duplication of overlapping controls.

- Information security policies and procedures not fully disseminated and implemented. PBGC is not able to effectively enforce compliance for all needed security awareness training. PBGC will be using an automated tool, the Talent Management System, to provide security awareness and role-based training.

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; revised date: August 31, 2015)**

  - 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; revised date: August 31, 2015)**

  - 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; revised date: August 31, 2015)**

[1] PBGC updated the number of common security controls identified from 130 to 208.

- Document and execute the details of the specific actions needed to complete and confirm the design, implementation, and operating effectiveness of all 208[2] 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; revised date: August 31, 2015)**

- 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; revised date: August 31, 2014)**

- Implement an effective review process to validate the completion of the SA&A[3] packages for all major applications. The review should not be performed by an individual associated with the performance of the SA&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; revised date: TBD)****

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

- Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the SA&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; revised date: TBD)****

- Implement an independent and effective review process to validate the completion of the SA&A packages for all major applications. **(OIG Control # FS-08-03-M-A) (PBGC scheduled completion date: June 30, 2013; revised date: August 31, 2014)**

- Implement a documented, independent and effective review process to validate the completion of the SA&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-M-B) (PBGC scheduled completion date: September 30, 2012; revised date: August 31, 2014)**

- 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; revised date: TBD)***

---

[2] PBGC updated the number of common security controls identified from 130 to 208.

[3] The Assessment and Authorization (A&A) now Security Assessment and Authorization (SA&A)

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 past decentralized approach to system development, system deployments, and configuration management created an environment that lacks a cohesive structure in which to implement co*ntro*ls 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 and Procedures* consistent with NIST SP 800-53, Rev 3. PBGC has developed and is implementing additional policies and procedures, including deploying technical and configuration management tools. PBGC is in the process of procuring, implementing and deploying technical tools 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 Patch and Vulnerability Management Group (PVMG, formerly the Tiger Team) focus on system scanning and vulnerability management, support PBGC's capability to carefully document and validate system vulnerabilities and provide evidence as to the operating effectiveness of some technical common controls. PBGC updated and improved its processes and procedures in FY 2013, including issuing the:

- Infrastructure Configuration Management Plan (ICMP) on March 21, 2013;
- Updated Configuration Management (CM) Process and Standard Operating Procedure (SOP) on March 21, 2013;
- Business Change Management Process (BCMP) and SOP April 18, 2013; and
- Updated Change Advisory Board (CAB) Charter on February 21, 2013.

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.

Without appropriate access and configuration management controls, PBGC does not have assurance that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

The specific weaknesses we found that contributed to the material weakness were due to the lack of the following:

- Infrastructure and configuration management
- System configuration settings
- Database configuration
- Segregation of duties-restriction of access to production environment
- Recertification of user and system access
- Management of user, generic and dormant accounts
- Audit logging and security monitoring
- Business process controls

Each of these weaknesses is described below with accompanying recommendations.

- Infrastructure and configuration management. 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 inconsistently implemented across PBGC's general support systems. PBGC's three IT environments (development, test, and production) do not share common server configurations. PBGC's infrastructure does not adequately segregate the production, development, and testing environments. The current environment requires additional time for the maturity of implemented technical controls, processes and procedures for the full implementation of an effective application development and change control program. PBGC has made improvements in developing and implementing baseline configuration management controls. In FY 2013, PBGC updated its Configuration Management Process and SOPs to include the use of technologies to support the Configuration Verification and Audit activity. Also, PBGC is in the process of institutionalizing the continuous monitoring aspect of configuration management for its systems.

  Recommendations:

  - 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; revised date: June 15, 2015)**

  - 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; revised date: December 15, 2013)**

- Establish baseline configuration standards for all of PBGC's systems. **(OIG Control # FS-09-13) (PBGC scheduled completion date: October 31, 2013; revised date: March 15, 2015)**

- 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; revised date: March 15, 2015)**

- 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; revised date: August 30, 2015)**

- 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; revised date: August 15, 2014)**

- System configuration settings. 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 PBGC's Information Security Policy (formerly IAH). PBGC's past 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. The failure to follow secure build standards and reassign or remove un-owned 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. In FY 2013, PBGC began the implementation of standards and procedures, deploying automated tools and enhanced infrastructure controls to more consistently apply authentication controls. Implementation and deployment of these controls now require time to mature in PBGC's environment, and prove their effectiveness.

  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 PBGC Information Security Policy (formerly 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; revised date: March 15, 2015)**

- Database configuration. 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. In FY 2013, PBGC updated its Configuration Management Process and SOPs to include the use of technologies to support the Configuration Verification and Audit activity. PBGC has started to replace its non-standard, End-of-Service-Life server infrastructure with standardized, secure server images. PBGC also established in FY 2013, approved baseline configurations for a majority of its production databases and networking devices. PBGC reported several accomplishments. It is beginning to use its newly acquired automated reporting capabilities to continuously monitor and address identified deviations from the established configuration baselines. Manual reporting SOPs are being implemented for cases where automation is not possible. It has begun institutionalizing the monthly review of automated and manual compliance reports to support its continuous monitoring process.

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; revised date: March 15, 2015)**

- 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; revised date: March 15, 2015)**

- Segregation of duties-restriction of access to production environment. 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. In some instances access cannot be restricted; PBGC is in the process of implementing compensating controls to restrict developer's access. PBGC has improved the process for granting access to its network and applications by updating the Network & Workspace Access, Transfer, and Modification processes to enhance the access approval workflow. However, PBGC has not fully resolved infrastructure design issues. PBGC is in the process of implementing technical and automated controls, but these enhanced configuration controls have not matured to ensure developer's access is properly restricted. The 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; revised date: January 3, 2014)**

Recertification of user and system access. The OIT recertification process remains incomplete and does not include all user and system access 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. In FY 2013, we noted that access account recertification packages were not complete for all systems. The account recertification for some systems did not include the approved user list, and in other systems, did not include the signed recertification letter. 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; revised date: December 31, 2013)**

- Management of user, generic and dormant accounts. PBGC's policies and practices have not effectively restricted the addition of unnecessary generic accounts to systems in production. 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. PBGC has taken action to review generic accounts in the general support systems (GSS), removing those that are unnecessary, and approving those that are necessary. For example, PBGC introduced automated tools in its GSS to more effectively control the dormant account process. The new automated process requires time to mature to prove its effectiveness. However, more work is needed to ensure that all unnecessary and generic accounts are removed. The 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; revised date: October 31, 2014)**

- 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; revised date: August 31, 2014)**

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

- Audit logging and security monitoring. Periodic logging and monitoring of security related events for PBGC's applications were inadequate for the Consolidated Financial System (CFS), Premium Accounting System (PAS), Participant Records Information System Management (PRISM), and Integrated Value of Future Benefits (IPVFB) systems. PBGC's IT infrastructure consists of multiple legacy systems and application that do not have a coherent architecture for management and security. Specific controls are not in place to ensure adequate consideration of the potential security impacts due to 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 PBGC has standardized the auditable events common to all GSS infrastructure components. PBGC has documented and approved Audit Configuration Settings for how to configure auditable events on particular devices, including servers, databases, communications devices, etc. PBGC is currently implementing the configuration of these auditable events across all devices. A Central Audit Logging solution has been selected and procurement is in process. This solution will act as a central repository for the collection, querying and reporting functions to support PBGC's Continuous Monitoring program.

  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; revised date: August 31, 2015)**

- Application- access controls. 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:

  - Establish unique accounts for each user in TeamConnect. **(OIG Control # FS-11-02) (PBGC scheduled completion date: September 30, 2012; revised date: TBD)****

  - Restrict developer's access to production. **(OIG Control # FS-11-03) (PBGC scheduled completion date: March 31, 2012; revised date: TBD)***

  - 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: December 30, 2012; revised date: December 31, 2013)**

  - Implement compensating controls for log and review of changes made by powerful shared accounts. **(OIG Control # FS-11-05) (PBGC scheduled completion date: December 31, 2012; revised date: December 31, 2013)**

- Business process controls. The Policy, Research and Analysis Department (PRAD) uses spreadsheets in the determination of the interest rate factor used for calculating PBGC's liabilities for future benefits, that do not have adequate controls over access to data, information security and changes. A contributing factor that sets the stage for this deficiency is PRAD's lack of adequate documentation of its process and procedures to ensure that spreadsheet calculations and other activities can be repeated by unassociated officials.

  Recommendations:

  - Document all key processes and procedures used by PRAD in its calculations and other activities. **(OIG Control Number FS-13-03)**

  - Document controls for managing spreadsheets to ensure their integrity and completeness. **(OIG Control Number FS-13-04)**

  - Document and maintain an inventory of spreadsheets used by PRAD. **(OIG Control Number FS-13-05)**

  - Develop, document and maintain processes and procedures to ensure that only current and approved versions of spreadsheets are being used by creating standardized naming conventions and directory structures. (**OIG Control Number FS-13-06)**

  - Develop, document and implement controls to consistently secure information embedded in spreadsheets, and limit access to spreadsheets to those with business needs. **(OIG Control Number FS-13-07)**

4. Integrated Financial Management Systems

The risk of inaccurate, inconsistent, and redundant data is increased because PBGC lacks a single integrated financial management system. Part of the system requires manipulation and the use of manual procedures to upload (1) plan PVFB liabilities; (2) the commingled funds monthly trial balance summary journal; and (3) the monthly journal entry for the premium financial activity.

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. *OMB's Core Financial System Requirements* establishes mandatory financial management system performance goals applicable to all financial management systems. These goals include providing timely, reliable, and complete financial management information for decision making at all levels of government; and providing for "one-time" data entry and reuse of transaction data to support downstream integration, interfacing, or business and reporting requirements.

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 either have been abandoned (such as the suspension of

work on the Premium and Practitioner System to replace the Premium Accounting System or have been ineffective in leading to the integration of its financially significant systems.

PBGC has made progress in implementing an integrated financial system. However, the implementation has not been completed. The specific weaknesses that contributed to the significant deficiency are as follows:

- Implementation of the Premium and Practitioner System (PPS). Major work remains to be completed to provide PBGC with integrated financial management capabilities. By December 2013, PBGC plans to implement the Premium and Practitioner System. With PPS, the Corporation will be integrated with the Oracle eBusiness Suite COTS solution used for PBGC's Consolidated Financial Systems.

- Lack of automated interface. Manual intervention is required to import the IPVFB plan liabilities into the Trust Accounting System (TAS). Within TAS, the plan liabilities comma separated values (CSV) file is manually uploaded into TAS for processing. A similar procedure is applied for uploading the State Street Commingled Plans' monthly trial balance summary journal into TAS.

PBGC's FY 2013 accomplishments included implementation of the Trust Accounting System, an externally-hosted, commercial-off-the-shelf investment accounting package. PBGC also upgraded the current PAS by completing unique enhancements for Pension Protection Act legislative changes and high priority functions. PBGC has also identified areas of focus for its future financial management 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 will be integrated with the Oracle eBusiness Suite COTS solution used for PBGC's Consolidated Financial Systems, and will replace the PAS in December 2013. The contract to upgrade and implement PPS was awarded in FY 2013. PPS will be upgraded and implemented in four releases – G/L Interface, Trading Community Architecture (TCA), 2014, and Customer Relationship Management (CRM). Certain PPS tasks are underway.

Recommendation:

- 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 September 30, 2013; revised date: September 30, 2014)**

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.

Calverton, Maryland
November 15, 2013

EXHIBIT I - Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendation Closed During FY 2013:

Recommendation	Date Closed	Original Report Number
FS-09-09	11/14/2013	AUD-2010-2/FA-09-64-2
FS-09-11	11/14/2013	AUD-2010-2/FA-09-64-2
FS-10-03	11/14/2013	AUD-2011-3/FA-10-69-2
FS-10-05	10/10/2013	AUD-2011-3/FA-10-69-2
FS-11-08	10/10/2013	AUD-2012-2/FA-11-82-2
FS-12-01	10/10/2013	AUD-2013-2/FA-12-88-2
FS-12-03	10/10/2013	AUD-2013-2/FA-12-88-2
FS-12-04	10/10/2013	AUD-2013-2/FA-12-88-2

Open Recommendations as of September 30, 2013:

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-M-A	AUD-2009-2/FA-08-49-2
FS-08-03-M-B	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 **	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-09-12	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

Recommendation	Report
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-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-11-09	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
FS-12-02	AUD-2013-2/FA-12-88-2
FS-12-05 *	AUD-2013-2/FA-12-88-2
FY Ended September 30, 2013	
FS-13-01	AUD-2014-3/FA-13-93-2
FS-13-02	AUD-2014-3/FA-13-93-2
FS-13-03	AUD-2014-3/FA-13-93-2
FS-13-04	AUD-2014-3/FA-13-93-2
FS-13-05	AUD-2014-3/FA-13-93-2
FS-13-06	AUD-2014-3/FA-13-93-2
FS-13-07	AUD-2014-3/FA-13-93-2

* PBGC has not established a revised completion date.

** PBGC submitted documentation to close this recommendation. The auditors determined that further management clarification or corrective action was needed. PBGC needs to provide a revised completion date based on the OIG's feedback.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2013 and 2012 Financial Statements

Audit Report AUD-2014-3 / FA-13-93-2

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 12, 2013

To: Deborah Stover-Springer
Acting Inspector General

From: Josh Gotbaum
Director

Subject: Response to Draft FY 2013 Internal Control Report

Thank you for the opportunity to comment on the draft FY 2013 internal control report. We are in agreement with the findings in this year's report. We also agree with the recommendations, on the understanding that the recommended spreadsheet controls pertain solely to the aspect of PRAD's work relevant to the financial statements—the development of the interest factor. The attachment to this memorandum provides details regarding our planned corrective actions.

We are pleased that your report recognizes the many corrective actions made in benefits administration, including the improvements to the operations manual, the issuance of the records management manual, the development of the staff training materials, and the updating of the technical reference guides. We also appreciate the acknowledged improvements being made in addressing IT security through deploying tools, acquiring staff support, and developing new approaches within the National Institutes of Standards and Technology Risk Management Framework. We are committed to continued advances both in operations and IT.

With respect to the agreed-upon recommendations from prior years, we continue to make noteworthy progress. We have implemented new leadership in both the benefits administration and information technology areas since these controls issues were reported. We have established detailed corrective action plans to address the areas needing stronger controls and have regularly reported on the progress both within management and to your office, recommendation by recommendation.

As we work to address both the new and remaining prior recommendations, we will continue to provide your office with evidence of the corrective actions taken. We look forward to working with you to make PBGC an even better agency in service to millions of Americans.

Attachment

cc:

Patricia Kelly
Alice Maroni
Ann Orr
Jioni Palmer
Sanford Rich
Judith Starr
Martin O. Boehm
Christopher Bone
Philip R. Langham
Barry West
Theodore J. Winter

Benefits Payment Administration Department

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

   PBGC Response: PBGC agrees and is already working to address the specific errors raised and others we have identified to improve the related controls that help prevent similar future exceptions.

2. **OIG Recommendation:** PBGC should develop and implement improvements to the BAPD Systems (ACT and the Integrated Present Value of Future Benefits (IPVFB) systems to:
   - Record and value separate benefit components payable under different annuity forms
   - Record and value anticipated future benefit amount changes
   - Value temporary joint and survivorship (J&S) benefits.

   PBGC Response: PBGC agrees. We are fully engaged in the analysis and development of improvements to our systems.

BAPD progress on prior recommendations: As the draft report indicates, BAPD has made substantial progress over the past year in addressing earlier findings. An example of that progress is the independent review by a well-known CPA firm that we sponsored for our asset valuation procedures. We enlisted the aid of a second independent major CPA firm to consult on specific areas of the procedures. Both firms helped to train our staff auditors and managers on new procedures. We also introduced new contract language to ensure that contractors that support our asset evaluations will themselves be evaluated. Moving forward, we will be gathering and sharing with OIG evidence of the effectiveness of these actions.

Policy, Research and Analysis Department

"The Policy, Research and Analysis Department (PRAD) uses spreadsheets in the determination of the interest rate factor used for calculating PBGC's liabilities for future benefits that do not have adequate controls over access to data, information security and changes. A contributing factor that sets the stage for this deficiency is PRAD's lack of adequate documentation of its processes and procedures to ensure that spreadsheet calculations and other activities can be repeated by unassociated officials." (p. 14)

3. **OIG Recommendation:** Document all key processes and procedures used by PRAD in its determination of the interest rate factor used in calculating PBGC's liabilities for future benefits.

   PBGC Response: We agree that it is important to have documented key processes and procedures for the determination of the interest rate factor and have done much in that direction over the past year. For example, in April 2013, we provided the OIG with a copy of a newly-developed *PBGC Interest Factors Procedures Manual* as well as

completed workpapers and management review checklists supporting the development of the quarterly interest rate factor for the second quarter of FY 2013. We will be happy to discuss reasonable additional documentation.

4. **OIG Recommendation:** Document controls for managing spreadsheets to ensure their integrity and completeness.

   PBGC Response: We agree that certain critical spreadsheets related to the development of the interest factor require documented controls to improve their management.

5. **OIG Recommendation:** Document and maintain an inventory of spreadsheets used by PRAD.

   PBGC Response: We agree to document and maintain an inventory of the spreadsheets used by PRAD to develop the interest factors used to determine PBGC liabilities for future benefits and are taking action in this direction.

6. **OIG Recommendation:** Develop, document processes and procedures to ensure that only current and approved versions of spreadsheets are being used by creating standardized naming conventions and directory structures.

   PBGC Response: We agree to develop and document policies and procedures used to calculate the interest factors that are used to determine PBGC liabilities for future benefits. We are already developing and documenting standardized naming conventions and directory structures for the related spreadsheets.

7. **OIG Recommendation:** Develop, document and implement controls to consistently secure information embedded in spreadsheets, and limit access to spreadsheets to those with business needs.

   PBGC Response: We agree to develop, document, and implement controls to consistently secure information embedded in spreadsheets pertaining to the calculation of the interest factors used to determine PBGC liabilities for future benefits. We are already developing and documenting the processes for requesting and making changes to these spreadsheets, as well as other related access, security, and integrity controls.

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