Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2014 and 2013 Financial Statements Audit

November 14, 2014

AUD 2015-3/FA-14-101-3

This page intentionally left blank.

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

November 14, 2014

To: Alice Maroni
Acting 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 2014 and 2013 Financial Statement Audit (AUD-2015-3/FA-14-101-3)

I am pleased to transmit the report prepared by CliftonLarsonAllen LLP resulting from their audit of the PBGC Fiscal Year 2014 and 2013 Financial Statements. The purpose of this report is to provide more detailed discussions of the specifics underlying the material weaknesses and significant deficiencies reported in the internal control section of the combined Independent Auditor's Report dated November 14, 2014 (AUD-2015-2 / FA-14-101-2).

Prior to issuance of this report, management agreed to all recommendations and expressed their commitment to addressing the recommendations contained in the report and to remediating the associated material weaknesses and significant deficiencies. However, the recommendations are still unresolved as PBGC management has not established completion dates for the recommendations. The Inspector General Act requires that audit recommendations be resolved within a maximum of six months from report issuance. Within 30 days please provide a corrective action plan and an estimated completion date to the Office of Inspector General.

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

Attachment

cc: Edgar Bennett
Cathleen Kronopolus
Jioni Palmer
Ann Orr
Sanford Rich
Judith Starr
Barry West
Ted Winter
Marty Boehm

This page intentionally left blank.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2014 and 2013 Financial Statements

Audit Report AUD-2015-3 / FA-14-101-3

Contents

This page intentionally left blank.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2014 and 2013 Financial Statements

Audit Report AUD-2015-3 / FA-14-101-3

Acronyms

AED	Asset Evaluation Division
ASD	Actuarial Services Division
BAPD	Benefits and Payment Department
CFS	Consolidated Financial System
CPF	Comprehensive Premium Filing
CSAM	Cyber Security Assessment and Management
DOI	Date of Insolvency
DoPT	Date of Plan Termination
FISMA	Federal Information Security Management Act
FIPS	Federal Information Processing Standards
FOD	Financial Operations Department
FY	Fiscal Year
GAB	General Accounting Branch
IAB	Investment Accounting Branch
ISA	Interconnection Security Agreements
IT	Information Technology
IPVFB	Integrated Present Value of Future Benefits
NCA	Non-Commingled Assets
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
ONR	Office of Negotiation and Restructuring
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
PPS	Premium and Practitioner System
PRAD	Policy, Research and Analysis Department
PVFB	Present Value of Future Benefits
PV NRFFA	Present Value of Nonrecoverable Future Financial Assistance
RMF	Risk Management Framework
SA&A	Security Assessment and Authorization
SP	Special Publication
SPBR	Small Plan Bulk Reserve
TA	Trust Accountants
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 2014 and 2013 Financial Statements

Audit Report AUD-2015-3 / FA-14-101-3

Section I

Independent Auditor's Report

This page intentionally left blank.

CliftonLarsonAllen

CliftonLarsonAllen LLP
CLAconnect.com

Supplemental Report on Internal Control Report

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, 2014, 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, contracts and grant agreements and have issued our audit report thereon dated November 14, 2014 (see Office of Inspector General (OIG) report AUD 2015-2/FA-14-101-2).

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 Independent Auditor's Report on PBGC's fiscal year (FY) 2014 financial statements, we identified certain deficiencies in internal control that we consider material weaknesses and other deficiencies that we collectively consider to be a significant deficiency. The purpose of this report is to provide more detailed information on these deficiencies.

Summary

PBGC protects the pensions of approximately 41 million workers and retirees in nearly 24 thousand private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of the Benefits Administration and Payment Department (BAPD), Financial Operations Department, and information technology (IT). Internal controls over these operations are essential to ensure the confidentiality, integrity, and availability of critical financial and operational data while mitigating the risk of errors, fraud, and other illegal acts.

The establishment of a robust internal control framework and the implementation of the appropriate internal control activities are essential to PBGC operations. Internal controls include the processes and procedures that PBGC management has placed into operation to ensure that the programs achieve their intended results; resources used are 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 reduce financial reporting and operational risks to PBGC as a whole, active involvement from PBGC's senior leadership in the monitoring and response to such risks is needed throughout each fiscal year.

In our Independent Auditors' Report, we identified the following material weaknesses for FY 2014:

1. BAPD Management and Oversight
2. Entity-wide Security Program Planning and Management
3. Access Controls and Configuration Management

We also identified the following new issues which we considered to be significant deficiencies for FY 2014:

4. Financial Reporting
5. Present Value of Nonrecoverable Future Financial Assistance (PV NRFFA)

PBGC continued to remediate conditions that contribute to the previously identified deficiencies with its internal controls. We observed improvements to the BAPD operations and the IT environment. PBGC continued to lay the groundwork in the deployment of tools, acquisition of staff, and development of approaches that will enable PBGC to better manage the design, implementation, and operational effectiveness of its IT security controls. Also, PBGC continued to develop and implement procedures and processes for the consistent implementation of common security and configuration management controls to minimize security weaknesses. However, the agency is still developing and implementing corrective actions to some of these long-standing operational and IT security weaknesses, some of which are not scheduled for completion until FY 2018.

The following provides an overview of each of the findings identified in our report. We provide greater detail for each finding in Exhibit I.

1. BAPD Management and Oversight

BAPD's control weaknesses over their valuation of plan benefits and related liabilities continue to merit senior leadership's focus. Although BAPD initiated corrective actions to address control weaknesses, a number of control deficiencies remain and continue to pose significant risks to PBGC's operations. These control deficiencies include inaccurate calculation of plan participants' benefits, inaccurate financial reporting, and noncompliance with prescribed laws and regulations. BAPD's management has taken a multi-year approach to remediate control weaknesses, but significant challenges remain as it undergoes leadership changes and significant restructuring.

We continue to identify the following control deficiencies:

A. Calculation of the Present Value of Future Benefits (PVFB) Liability

The PVFB liability had errors that impacted the participant benefits and the related liability. Some of these errors were attributed to BAPD's systems (Integrated Present Value of

Future Benefits (IPVFB) and Spectrum) limitations and data entry errors. The internal control activities were ineffective in identifying these errors in the calculation of the PVFB liability.

B. Documentation to Support Benefit Calculations

We continued to observe that management could not provide appropriate documentation to support, substantiate, and validate the benefit calculation for certain participants in our sample. Documentation to support benefit calculations should be readily available for examination. This lack of documentation increases a risk of misstatement of the PVFB liability.

C. Valuation of Plan Assets and Benefits

In prior years, we found that PBGC did not properly determine the fair market value of certain assets of trusteed plans at the date of plan termination (DoPT) as required by its regulation. As a result of this deficiency in the assets valuation process, certain plan participant's benefits may have been misstated.

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 mitigate certain information system security control deficiencies. Though progress had been made, control deficiencies continued in FY 2014. These control deficiencies hindered PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure. The security management program should establish a framework and a continuous cycle for assessing risk, developing and implementing effective procedures, and monitoring the effectiveness of these procedures.

We continue to identify security control weaknesses in the following:

A. Security Management

An effective information security management program should have a framework and process for assessing risk, effective security procedures, and processes for monitoring and reporting the effectiveness of these procedures.

Though progress was made, PBGC did not completely establish and implement tools and processes needed to obtain performance measures and information on security progress to facilitate decision making and management, including:

- Finalizing metrics and security progress information to indicate the effectiveness of its security controls applied to information systems and supporting information security programs.
- Collecting, analyzing, and reporting all relevant performance-related data to facilitate decision making, improve performance, and increase accountability.

- Collecting all relevant performance data on implementation measures to determine the level of execution of its security policy; effectiveness/efficiency measures to evaluate results of security services delivery; and impact measures to assess business or mission consequences of security events.
- Demonstrating how implementation, efficiency, and effectiveness of its information system and program security controls contribute to the Corporation's success in achieving its mission.

B. Common Security Controls

Common security controls provide the foundation for the effectiveness of enterprise-wide system security operations. In FY 2014, PBGC continued to change its common controls, which did not allow adequate time for the controls to mature in the environment and operate effectively. Specifically, during FY 2014, PBGC consolidated its two general support systems which decreased the number of common controls from 208 to 118. However, PBGC did not document this consolidation of controls. In addition, the Corporation is considering adding 67 new controls to the set of common controls. Furthermore, PBGC did not communicate the new strategy and change in common controls to system owners of PBGC's major applications, who relied on these controls.

PBGC tested 108 of the 118 common controls for effectiveness. We found fifty-five of the common controls tested were effective and 53 common controls were ineffective.

C. Security Assessments and Authorization (SA&A)

In June 2014, PBGC consolidated multiple inventory lists into one (1) authoritative list to track the Federal Information Security Management Act of 2002 (FISMA) inventory, subsystem components, Interconnection Security Agreements (ISAs), and SA&A schedules. The FISMA inventory list is scheduled to be updated monthly. PBGC acknowledges that it will require time to demonstrate the effectiveness of the new process.

PBGC continued to enhance its SA&A quality control process to address weaknesses noted in prior years. In FY 2014, the Corporation performed a deeper analysis of their SA&A packages; standardized the quality control review approach; and determined the level of inspection to be performed. PBGC applied this enhanced quality control review process to one system and uncovered deficiencies which were resolved before the SA&A package was submitted and approved. PBGC plans to use this new quality control process to review future SA&A packages. Currently, three systems have not been authorized to operate, based on the SA&A process.

3. Access Controls and Configuration Management

Access controls and configuration management controls are an integral part of an effective information security management program. Access controls limit or detect inappropriate access to systems, protecting the data within them from unauthorized modification, loss or disclosure. Configuration management ensures changes to systems are tested and approved and systems are configured securely in accordance with policy.

Access controls and configuration management remain a systemic problem throughout PBGC. In FY 2014, PBGC submitted documentation and evidence to support the closure of fourteen (14) access and configuration management prior year recommendations. However, based on our current year testing, we could only close five (5) of these recommendations. The documentation provided for the nine (9) recommendations that will remain open did not demonstrate that controls were properly implemented, repeatable, and maintained. Furthermore, documentation in certain cases did not address the root cause of the weakness. Weaknesses in the PBGC IT environment contributed significantly to deficiencies in system configuration, segregation of duties, role-based access controls, and monitoring.

We continue to identify the following control weaknesses in access controls and configuration management. Specifically:

A. Configuration Management

Although PBGC has defined baseline configurations for its systems, tools, and applications, and modified common configuration management security controls, they require time to demonstrate operational effectiveness. Automated tools to manage configuration infrastructure are not fully operational. For FY 2014, unresolved vulnerabilities still remain in key databases and applications, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. Prior weaknesses in authentication parameters for general support systems and applications were not adequately addressed.

B. Access Controls and Account Management

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

1) Segregation of Duties

PBGC did not effectively restrict developers' access to production. We found that for one (1) of the seven (7) applications tested developers were provided more than read-only access to production. After PBGC was informed, PBGC removed the developers' access.

PBGC did not clearly define the duration and procedures surrounding the use of temporary access. Temporary/emergency access procedures did not establish a timeline and/or duration to remove the emergency access. Additionally, a risk acceptance form was created to address developers' temporary/emergency access to an application; however, the risk acceptance form did not clearly identify the timeframes for temporary/emergency access.

2) Account Management

Account Dormancy

PBGC's practice for disabling and removing dormant accounts were not in compliance with its policy. In FY 2014, PBGC assessed compliance with authentication and dormancy standards and found that automated controls were not implemented to enforce/adhere to PBGC's dormancy standards for twelve (12) major applications and five (5) sub-components of the General Support System.

For nine (9) of the major applications, risk acceptance forms addressed account configuration settings; however, eight (8) of them did not address account dormancy.

Generic Accounts

In FY 2013, we recommended that PBGC continue to remove unnecessary user and generic accounts. While PBGC established formal policies, PBGC did not provide evidence that it removed unnecessary user and generic accounts.

C. Incident Handling and Security Monitoring

We identified deficiencies in PBGC's Incident Response Program in our FY 2013 FISMA report. For FY 2014, we found that while PBGC had defined Incident Response Procedures, those procedures did not provide clear and detailed guidance on how to: monitor information systems; detect, identify, document, and report incidents; as well as when to elevate incidents. This lack of clear guidance had and may lead to future mismanagement of incidents.

PBGC purchased an automated tool to collect, analyze, search, and monitor information system security logs across the enterprise. This tool will enhance PBGC's detection of security events in applications, operating systems, databases, and network monitoring tools. However, this tool was not fully implemented. Specifically, this automated tool was not fully configured to collect data enterprise-wide. Progress was slow and not all information system owners provided a timeline for implementation.

4. Financial Reporting

The financial reporting process is at the forefront of preparing accurate and timely financial statements. Effective internal controls over financial reporting requires a strong environment under which all internal control components are implemented to meet the objectives of accurate financial reporting, compliance with laws and regulations and effective and efficient operations. Those responsible for executing the control activities should understand the control activities' purposes, and the activities should include monitoring staff execution, evaluating anomalous results for root cause, and documenting corrective action taken. The Financial Operations Department (FOD) is principally responsible for PBGC's accounting activities, financial reporting and maintenance of the financial and accounting systems. During FY 2014, we found that certain controls were not in place. These control deficiencies create risk and impact the

validity, completeness and accuracy of financial reporting. In FY 2014, we found a combination of deficiencies that collectively represent a new significant deficiency in financial reporting.

A. Lack of Controls over the Premium Process

PBGC lacks effective controls surrounding the completeness and accuracy of the premium revenue balance reported in the general ledger. In addition, the design of the manual reconciliation between the Premium and Practitioner System (PPS) premium subsidiary ledger to the general ledger is flawed. Finally, there is a system limitation with the PPS reporting functionality.

B. Lack of Controls over the Manual Processes

PBGC places reliance on a number of manual processes to record financial events in its general ledger. The inherent risks associated with manual processes require effective and reliable controls to mitigate such risks. We found that PBGC did not have effective internal controls throughout the fiscal year over manual journal entries and certain manual spreadsheets used to record financial transactions. Specifically, PBGC did not employ a sequential numbering scheme to assign journal entry numbers, and did not assign common numbers to routine or recurring journal entries to ensure that each routine or recurring entry is prepared each month. In addition, PBGC did not maintain a journal entry log to ensure that the journal entry population is complete and that no unauthorized entries have been made in Consolidated Financial System (CFS). Management recognized the benefit of sequentially numbering journal entries and a journal entry log and both tools were placed in operation by year-end.

PBGC did not have effective integrity and access controls over key financial spreadsheets that support the Corporation's financial reporting. In addition, PBGC did not have adequate integrity controls to guard against improper modification, access or degradation of key financial spreadsheets.

C. Monitoring controls over Non-Commingled Assets

PBGC's monitoring process over the valuation of the Non-Commingled Assets is deficient. We found those responsible for recording plan asset activities performed inadequate reviews of plan asset transactions recorded into the general ledger, processed untimely transfers of non-commingled assets to commingled assets, and did not maintain the case file documentation needed to support plan asset transactions.

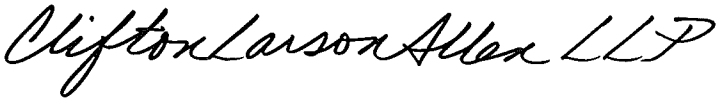
5. Present Value of Nonrecoverable Future Financial Assistance

The Present Value of Nonrecoverable Future Financial Assistance liability calculated by the Actuarial Services Division lacks a robust quality control review process to verify inputs to the IPVFB system. We identified five (5) control deficiencies during our September 30, 2014 testing that resulted in a new significant deficiency:

- Inappropriate use or misinterpretation of underlying documentation supporting the valuation;
- Errors in data entered into the IPVFB system;

- Misstatements in the expected employer withdrawal liability payments in the cash flows projection;
- Failure to use the most recent data available; and
- Missing documentation for IPVFB data.

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, 2014

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

1. BAPD 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, 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 Asset Evaluation Division (AED). The TPDs are responsible for capturing the participant data for benefit determinations, managing the participant and beneficiaries' benefit payments, and maintaining the pension plan and participant files. These files include documentation used to support the calculation of participant's benefit amounts and the corresponding pension liabilities recorded on PBGC financial statements. The AED is responsible for valuing plan assets of terminated single-employer pension plans and to determine the fair market value of those assets used to offset the plan liabilities assumed by the PBGC. ASD uses the underlying documentation maintained by the TPDs, as well as mortality tables and interest rate factors, as key inputs to calculate the present value of future benefits liabilities recorded on PBGC's financial statements.

Over the past two years, BAPD made progress to remediate control weaknesses. These efforts included extensive analyses primarily focused on the accurate calculation of plan participant's benefits and valuation of the associated liability. The results of the analyses support BAPD management's refinement to current practices and policies as well as organizational changes to correct these deficiencies. However, we found that challenges within the BAPD still remain.

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 identified:

- Errors caused by system limitations or programming flaws.
- Documentation procedures were not followed for plan terminations and documentation procedures used for system maintenance were inadequate.
- Data entry errors and inaccurate use of plan data provisions.

Using a statistically-based sampling technique, we identified approximately 12% 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 $70 billion at September 30, 2014, had an estimated range of an approximately $44 million understatement to $340 million overstatement and a point estimate of a $148 million overstatement. These long standing deficiencies in BAPD processes impede management's ability to accurately calculate valuations for some participant's benefits and related future liabilities.

Documentation to Support Benefit Calculations

BAPD's documentation used to support the calculation of the PVFB continues to be a significant challenge. During our testing at June 30 and September 30, BAPD was not able to provide the documentation needed to fully support liability calculations for some samples. The lack of appropriate documentation 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 documentation deficiencies in BAPD, including the need to require archiving source documents, implementation of controls to ensure monitoring and enforcement of documentation procedures, and improve the training for persons tasked with calculating and reviewing benefit determinations. BAPD continues to strengthen their controls around the benefit calculations. However, these deficiencies remain and the likelihood of inaccurate valuation of plan liabilities reported in the financial statements continues to exist. Inaccurate plan liabilities 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:

- Promptly correct errors in benefit calculations and data entries identified by the auditors during FY 2014. **(OIG Control # FS-14-01)**

- PBGC should perform an analysis to identify risks associated with a lack of documentation to support all participants' benefit calculations and assess the impact to the calculations and related liability. **(OIG Control # FS-14-02)**

- Upon completion of analysis, PBGC should develop a policy to finalize management's position on the financial impact of the lack of documentation issue and any actions that will be taken to address this systemic issue. The policy should also document any residual risk that it may elect to accept. **(OIG Control # FS-14-03)**

- Develop and document a risk assessment of the BAPD's entire operations. The risk assessment should include the identification of all the root causes of the issues identified by the auditors and ASD. PBGC should monitor the implemented corrective actions. The materiality thresholds used should be reasonable. **(OIG Control # FS-14-04)**

- Review known case 187419 (Allegheny Health) in light of the calculation exception for Sample 27 and determine if other plan participants are receiving incorrect benefits due to the miscalculation of the Retirement Service Credit Fraction. PBGC should insure that all data and calculation methodology is properly stored and documented. Interim calculations of data elements used to determine the Termination Benefit should be archived with the actuarial case report and the methodology described the actuarial case memo. For sample 27, the data used to determine the Retirement Service Credits, which is the basis for the Retirement Service Credit Fraction calculation was completed outside of the valuation spreadsheet and the methodology and data were not archived. **(OIG Control # FS-14-05)**

- Expand modernization efforts to Spectrum and the IPVFB systems to:
  1. Value the actual popup benefit for Joint and Survivor Popup annuity forms.
  2. Value non-level and surviving spouse benefits without the need for supplemental tables.
     (OIG Control # FS-14-06)

- Ensure that deviations from established procedures should be properly documented and approved. **(OIG Control # FS-14-07)**

- Continue to promptly correct the errors in its calculations identified by the auditors during the FY 2013 testing of the IPV. **(OIG Control # FS-13-01) (PBGC revised completion date: December 31, 2018)**

- PBGC should continue to develop and implement improvements to the BAPD Systems (Spectrum and the IPVFB) to:
  1. Record and value separate benefit components payable under different annuity forms.
  2. Record and value anticipated future benefit amount changes.
  3. Record and value temporary joint and survivorship benefits. **(OIG Control # FS-13-02) (PBGC scheduled completion date: December 31, 2018)**

- 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 # FS-12-02) (PBGC revised completion date : December 31, 2015)***

- 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 was used to support benefit payments and IPVFB liabilities. **(OIG Control # FS-12-05) (PBGC revised completion date: January 31, 2015)***

- Ensure that adequate documentation was 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 revised date: December 31, 2015)***

- 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) (PBGC revised date: September 30, 2014) ***

Valuation of Plan Assets and Benefits

BAPD has undertaken significant efforts to revalue assets for certain pension plans trusteed by PBGC. The fair market value of a pension plan's assets at the date a plan was terminated is an essential factor to determine the retirement benefit amounts owed to plan participants. In FY 2014, BAPD revised their plan asset valuation procedures to include a contractor checklist to aid in the quality review process and to ensure contractor performance meets the statement of work requirements and objectives. In addition, the AED is refining the quality review process for plan asset valuations to be performed by Federal employees.

Although certain corrective actions were implemented, internal control weaknesses continue to deserve management's continued focus. BAPD's quality control review process over plan asset valuations conducted by Federal employees and the new plan asset evaluation process has yet to mature. Furthermore, BAPD did not complete the re-work of the plan asset valuations based

on its risk-based approach to determine whether participant's benefits require any adjustment. Until these plan asset valuations are completed, significant risks to the reliability of participants' benefit determinations and PBGC reported liability remain. The plan asset valuations are expected to be completed in FY 2015 and thereafter.

Recommendations:

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

- Refine 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 revised date: June 30, 2015)***

- Continue to identify those plans that might potentially have a pervasive misstatement to the financial statements if DoPT asset values were originally misstated. Management should then re-evaluate the DoPT asset values for those identified plans and consider the impact of any known differences on the financial statements. **(OIG Control # FS-11-09) (PBGC revised date: September 30, 2015)***

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 2014, 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.

FISMA requires each federal agency to establish an agency-wide information security program to provide security to the information and information systems that support the operations and assets of the agency, including those managed by a contractor or other agency. OMB Circular No. A-130, Appendix III, *Security of Federal Automated Information Resources,* requires agencies to implement and maintain a program to assure that adequate security is provided for all agency information collected processed, transmitted, stored, or disseminated in general support systems and major applications.

A. Security Management

PBGC is still in the process of establishing and implementing tools and processes needed to obtain performance measures and information on security progress to facilitate decision making and management of PBGC's IT assets. PBGC's FISMA compliance, security management, and vulnerability remediation and automated reporting tool, Cyber Security

Assessment Management is still in pilot stage. The FY 2014-2018 *Information Technology Strategic Plan*, finalized in December 2013, prioritizes the security of PBGC's IT as its number one goal to ensure confidentiality, availability, and integrity of systems and data. The Chief Information Officer (CIO) also had regular meetings with key stake holders and decision-makers on IT security issues. However, PBGC did not complete the following security performance measure tasks to provide critical security management information:

- Finalize metrics and security progress information to indicate the effectiveness of its security controls and supporting information security programs.
- Collect, analyze and report all relevant performance-related data to facilitate decision making, improve performance and increase accountability.
- Collect all relevant performance data on implementation measures to determine the level of execution of its security policy; effectiveness/efficiency measures to evaluate results of security services delivery; and impact measures to assess business or mission consequences of security events.
- Demonstrate how implementation, efficiency and effectiveness of its information system and program security controls contribute to the Corporation's success in achieving its mission.

Federal entities are required to employ a risk-based approach to security management. This approach is based on the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). NIST defines an effective risk management framework as the process of managing risks to organizational operations (including mission, functions, image, and reputation). The following must be completed to have a comprehensive risk-based approach to security management: (i) conducting a risk assessment; (ii) implementing a risk mitigation strategy; and (iii) employing techniques and procedures for the continuous monitoring of the security state of the information system.

Risk management is progressive, proactive, focused on synergistic solutions, and based on formal frameworks and methodologies. NIST's RMF illustrates general steps that should be taken to protect the organization and its mission. Managing the risk associated with information systems (including technology and the people, processes, and environment surrounding the technology) is one part of that overall protection.

The RMF emphasizes building information security into the culture and infrastructure of an organization. Achieving this goal starts with understanding, commitment, guidance, and involvement from senior leadership. It requires education and accountability at appropriate levels, and depends on communication and trust throughout the organization. Only then can specific security authorization efforts be carried out to protect the organization and its mission.

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 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 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 revised date: August 31, 2015)***

B. Common Security Controls

Common security controls provide the foundation for the effectiveness of enterprise-wide system security operations. In FY 2014, PBGC continued to change its common controls, which did not allow adequate time for the controls to mature in the environment and operate effectively. Specifically, during FY 2014, PBGC consolidated its general support systems from two (2) to one (1), which decreased the number of common controls from 208 to 118. However, PBGC did not document this consolidation of controls. In addition, the Corporation is considering adding 67 new controls to the set of common controls. Furthermore, PBGC did not communicate the new strategy and change in common controls to system owners of PBGC's major applications, who relied on these controls.

PBGC tested 108 of the 118 common controls for effectiveness. Fifty-five of the common controls tested were found to be effective and 53 common controls were ineffective. Common controls are security controls that are inherited by one or more information systems within PBGC. Common controls promote more cost-effective and consistent information security across the organization and can also simplify risk management activities. Common controls provide a security capability for multiple information systems. Common controls are identified by the Chief Information Officer and/or Senior Information Security Officer in collaboration with the information security architect and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring.

Common control providers are responsible for: (i) documenting common controls in a security plan (or equivalent document prescribed by the organization); (ii) ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization; (iii) documenting assessment findings in a security assessment report; (iv) producing a plan of action and milestones (POA&M) for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls); (v) receiving authorization for the common controls from the designated authorizing official; and (vi) monitoring common control effectiveness on an ongoing basis.

Common controls that are relied upon are documented within each information system security plan. Organizations are to ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls.

Recommendations:

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

C. Security Assessments and Authorization (SA&A)

In June 2014, PBGC consolidated its multiple inventory lists into one (1) authoritative list to track the FISMA inventory, subsystem components, ISAs, and SA&A schedules. The FISMA inventory list is scheduled to be updated monthly. PBGC acknowledges that it requires time to demonstrate the effectiveness of the new process.

PBGC continued to enhance its SA&A quality control process to address weaknesses noted in prior years. Currently, 17 of the 20 major applications and general support systems have SA&As conducted; specifically, three major applications and general supports systems did not have current SA&As. In FY 2014, the Corporation performed a deeper analysis of their SA&A packages, standardized the quality control review approach, and determined the level of inspection to be performed. The enhanced quality control review process was applied to only a single system. As a result of the enhanced quality control review process, deficiencies were uncovered which were resolved before the SA&A package was submitted and approved. The other 16 major applications and general support systems with SA&As were utilizing the legacy quality control process. PBGC plans to use this new quality control process to review future SA&A packages.

FISMA requires that each agency develop, maintain and annually update an inventory of major information systems (i.e., major applications and general support systems) operated by the agency or under its control. Federal Information Processing Standards Publication 200 (FIPS 200), *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. Organizations first determine the security category of their information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST SP800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, requires that security authorization packages be prepared for each major information system for official authorization. The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to

make risk-based authorization decisions. The security authorization process is an inherently Federal responsibility and therefore, authorizing officials must be federal employees. OMB policy requires that organizations conduct ongoing authorizations of information systems by implementing continuous monitoring programs. If the agency has established continuous monitoring programs, this can satisfy three-year reauthorization requirements.

Recommendations:

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

- Implement an effective review process to validate the completion of the SA&A 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 revised date: June 30, 2015)***

- Implement an enhanced quality review process to 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 revised date: June 30, 2015)***

- 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 revised date: June 30, 2015)***

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

3. Access Controls and Configuration Management

Access controls and configuration management controls are an integral part of an effective information security management program. Access controls limit or detect inappropriate access to systems, protecting the data from unauthorized modification, loss or disclosure. Agencies should have formal policies and procedures and related control activities should be properly implemented and monitored. Configuration management ensures changes to systems are tested and approved and systems are configured securely in accordance with policy.

Access controls and configuration management remain a systemic problem throughout PBGC. In FY 2014, PBGC submitted documentation and evidence to support the closure of fourteen (14) access and configuration management prior year recommendations. However,

based on our current year testing, we noted that nine (9) of these recommendations were not closed. The documentation provided for these nine (9) recommendations did not demonstrate that controls were properly implemented, repeatable, and maintained. Furthermore, documentation in certain cases did not address the root cause of the weakness. Weaknesses in the PBGC IT environment contributed significantly to deficiencies in system configuration, segregation of duties, role-based access controls, and monitoring.

A. Configuration Management

While PBGC has defined baseline configurations for its systems, tools, and applications, the implementation of processes to ensure compliance with these baselines did not mature. Common configuration management security controls were modified and changed as part of the development of a more coherent strategy to mitigate systemic weaknesses in all environments. These controls require time to mature to demonstrate their operational effectiveness. PBGC continues to procure, implement, and deploy tools and processes to better manage the configuration of common operating platforms, servers and devices, and compliance to the defined baselines. 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. Unresolved vulnerabilities still remain in key databases and applications, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. Weaknesses noted in authentication parameters for general support systems and applications were not adequately addressed.

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. Systems with secure configurations are less vulnerable and are better able to thwart network attacks.

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.

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, CM-2 – Baseline Configuration requires that organizations develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

NIST SP 800-53, Revision 4, IA-5 – Authenticator Management states the organization manages information system authenticators by establishing initial authenticator content for authenticators defined by the organization; ensuring that authenticators have sufficient strength of mechanism for their intended use; establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; changing/refreshing authenticators on an organization-defined time period by authenticator type; and protecting authenticator content from unauthorized disclosure and modification.

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 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 revised date: December 15, 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 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 revised date: March 15, 2015)***

- Implement controls to remedy vulnerabilities identified 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 revised date: March 15, 2015)***

- 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 document their risk acceptance. **(OIG Control # FS-09-17) (PBGC revised date: August 31, 2014)***

- 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)**

B. Access Controls and Account Management

1) Segregation of Duties Among IT Environments

PBGC did not effectively restrict developers' access to production. Specifically, we noted that there were developers with access to production for one (1) application of a sample of seven (7) applications tested. After PBGC was informed, PBGC removed the developers' access.

PBGC did not clearly define the duration and procedures surrounding the use of temporary/emergency access. During FY 2014, temporary/emergency and perpetual access was utilized in a similar manner. Specifically, we noted that in FY 2014, PBGC updated the *PBGC System Privilege Standard*, which allows developers access to production on a temporary/emergency basis. However, the standard did not establish a timeline and/or duration to remove the temporary/emergency access. Additionally, a risk acceptance form was created to address developers' temporary/emergency access to an application; however, the risk acceptance form did not clearly identify the timeframes for temporary/emergency access.

NIST SP 800-53, Revision 4, AC-5 – Separation of Duties specifies that organizations should separate duties of individuals as necessary, to prevent malevolent activity without collusion and implement separation of duties through assigned information system access authorizations. An example of separation of duties include different individuals perform information system support functions (e.g. system management, systems programming, configuration management, quality assurance and testing, network security, etc.). In addition, NIST SP 800-53, Revision 4, CM-5 – Access Restrictions for Change requires organizations to define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Access restrictions for change also include software libraries.

Recommendations:

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

- Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10) (PBGC revised date: January 3, 2014)***

- Restrict developers' access to production (TeamConnect). **(OIG Control # FS-11-03) (PBGC revised date: TBD)****

2) Account Management

Account Dormancy

PBGC's practice for disabling and removing dormant accounts was not in compliance with its policy, *PBGC Access Control Standard,* which required that accounts be disabled after a defined period of inactivity and deleted after a defined period. In FY 2014, PBGC conducted an assessment of authentication and dormancy standards compliance. This assessment noted that automated controls were not implemented to enforce/adhere to PBGC's dormancy standards for twelve (12) major applications and five (5) sub-components of the General Support System.

Risk acceptance forms existed for nine (9) of the major applications that addressed account configuration settings. However, we noted that eight (8) of the major applications' Risk Acceptance Forms did not directly address account dormancy. Once notified, PBGC revised these Risk Acceptance Forms to address account dormancy.

NIST SP 800-53, Revision 4, AC-2 - Account Management states that the information system should automatically disable inactive accounts after a determined period of inactivity.

Generic Accounts

In FY 2013, we recommended that PBGC continue to remove unnecessary user and generic accounts. While PBGC has established formal policies, PBGC did not provide any documentation to demonstrate progress in the removal of unnecessary user and generic accounts from its systems. Failure to identify and remove unnecessary accounts could result in PBGC's systems being at an increased risk of unauthorized access/modification/deletion of sensitive system data and/or participant information.

NIST SP 800-53, Revision 4, IA-4 - Identifier Management requires that organizations manage individual identifiers by uniquely identifying each individual user.

Recommendations:

- Apply controls to remove/disable inactive and dormant accounts after a specified period for the affected systems in accordance with the PBGC Information Security Policy (formerly Information Assurance Handbook - IAH). **(OIG Control # FS-07-12) (PBGC revised date: TBD)****

- Continue to remove unnecessary user and generic accounts. **(OIG Control # FS-07-08) (PBGC revised date: October 31, 2014)***

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

C. Incident Handling and Security Monitoring

We identified deficiencies in PBGC's Incident Response Program in our FY 2013 FISMA report. For FY 2014, we found that while PBGC defined Incident Response Procedures, those procedures did not provide clear and detailed guidance on how to monitor information systems; detect, identify, document, and report incidents; as well as when to elevate incidents. This lack of clear guidance has and may lead to future mismanagement of incidents.

PBGC purchased an automated tool to collect, analyze, search, and monitor information system security logs across the enterprise. However, this tool was not fully implemented. Specifically, this automated tool was not fully configured to collect data enterprise-wide. Progress was slow and not all information system owners provided a timeline for implementation. This tool enhances PBGC's detection of security events in applications, operating systems, databases, and network monitoring tools.

Effective incidence response starts with audit and monitoring activities that include regular collection, review, and analysis of auditable events for indications of inappropriate or unusual activity. Essential controls include defining the required steps to thoroughly examine the activity, when elevation is required and to whom it must be reported. Automated mechanisms may be used to integrate audit monitoring, analysis, and reporting into an overall process for incident examination and response to suspicious activities. These automated controls are only one tool. They do not take the place of well-trained and well-supervised IT security professional staff who are implementing effective guidance in using the automated security monitoring tools.

Audit and monitoring controls can help security professionals routinely assess computer security, perform effective examinations during and after an attack, and even recognize an ongoing attack. Audit and monitoring technologies include network and host-based intrusion detection systems, audit logging, security event correlation tools, and computer forensics. Network-based IDSs capture or "sniff" and analyze network traffic in various parts of a network. On the other hand, host-based IDSs analyze activity on a particular computer or host. Both types of IDS have advantages and disadvantages. All Federal agencies are required to implement an information security program that includes procedures for detecting, reporting, and responding to security incidents.

We identified the following weaknesses in PBGC's access controls over incidence response that created substantial risk when an incidence occurs the exposures of sensitive and personally identifiable information (PII) will not be quickly identified and contained:

- Incident handling process was ineffective in monitoring, detecting, examining and reporting security incidents.
- Security incident policies and procedures were not reviewed annually in accordance with PBGC's policies.
- Incident handling process was not reviewed to ensure effectiveness of PBGC's security event categorization procedures and decision process, review of IDS logs, and other continuous monitoring activity.

- PBGC did not establish adequate guidelines for the contractors to execute in documenting, examining and reporting security incidents to PBGC management. Further, management did not ensure that corrective actions were implemented to remediate security vulnerabilities disclosed.
- Prioritization factors were not developed for security incidents, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity and availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident).
- After a specific phishing event was identified by the OIG, no assessment was conducted to determine the adequacy of PBGC's current data loss prevention controls.
- After the identified event, controls were not developed and implemented to enhance PBGC's ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information.
- Directive IM 10-3, *Protecting Sensitive Information*, was not updated to provide updated guidance on protecting sensitive information.

NIST SP 800-53, Revision 4, IR-4 - Incident Handling requires the organization to implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

NIST SP 800-53, Revision 4, IR-5 - Incident Monitoring requires the organization to track and document information system security incidents.

NIST SP 800-53, Revision 4, IR-6 - Incident Reporting requires the organization personnel to report suspected security incidents to the organizational incident response capability within an organization-defined time period; and report security incident information to organization-defined authorities.

Recommendations:

- Update and document the security event categorization procedures and decision process to better define the thresholds where security events are categorized as suspicious and are recorded in a ticketing system as an incident for escalation and further analysis. **(OIG Control # FS-14-08)**

- Establish a periodic review (at least quarterly) process for contractor's compliance, including the execution of PBGC's security event categorization procedures and decision process, review of IDS logs, and other continuous monitoring activity. **(OIG Control # FS-14-09)**

- Ensure that security incidents are documented, investigated, reported to federal management, and corrective actions implemented to remediate security vulnerabilities. **(OIG Control # FS-14-10)**

- Develop factors to prioritize security incidents, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact

of the incident (e.g., effect on the confidentiality, integrity, and availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident). **(OIG Control # FS-14-11)**

- Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk. **(OIG Control # FS-14-12)**

- Develop and implement controls to enhance PBGC's ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information. **(OIG Control # FS-14-13)**

- Review, update, and approve Directive IM 10-3, Protecting Sensitive Information. **(OIG Control # FS-14-14)**

- 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 revised date: August 31, 2015)**

4. Financial Reporting

The financial reporting process is at the forefront of preparing accurate and timely financial statements. Effective internal control over financial reporting requires a strong entity level management structure that focuses on all five components of internal control:

- control environment,
- control activities,
- risk assessment,
- information and communication, and
- monitoring.

In addition, strong internal control activities should be implemented to effectively meet the objectives of accurate financial reporting, compliance with laws and regulations and effective and efficient operations. Those responsible for executing the control activities should understand the control activities' purposes, and the activities should include monitoring staff execution, evaluating anomalous results for root cause, and documenting corrective action taken. At PBGC, the FOD is principally responsible for financial reporting including recording financial transactions and for the maintenance of the financial accounting systems.

During FY 2014, we found that certain controls were not in place. These control deficiencies create risk and impact the validity, completeness and accuracy of financial reporting. In response to some current year audit findings, management implemented corrective action prior to the end of the fiscal year. We found the combination of deficiencies that collectively represent a new significant deficiency.

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

A. Lack of Controls over the Reporting of Premium Income

Under Title IV of ERISA, PBGC generates income from the covered single-employer and multiemployer defined benefit pension plans that are required to pay premiums. Both types of plans pay a flat rate premium; the single-employer plans may also pay a variable rate premium based on a dollar threshold per participant of underfunding. In FY 2014, PBGC implemented the PPS, a new subsidiary financial system used to account for the premium income activities.

During FY 2014, we found the following premium income reporting deficiencies:

- PBGC does not perform a comprehensive analysis of key data inputs from the Form 5500 and the Comprehensive Premium Filing (CPF). All pension plans are required to file a Form 5500 annually to report specific data on plan activities. Both forms include plan participant counts and market value of the plan assets data, and are loaded into PPS. These inputs are essential to calculate the fixed rate and variable rate premiums. Comparing the data for significant variances and evaluating the root cause would be an effective control to identify premiums owed to PBGC. We found that management uses the electronic Form 5500 and CPF data to perform a limited comparison to match a defined benefit plan sponsor's Employer Identification Number/Plan Number. This analysis will not identify variances between key data inputs that may alert PBGC of improper premium filings.

- PBGC does not perform a comprehensive analysis over the premium data to determine the completeness and accuracy of premium income. During our June 30 interim test work, we found an error in the premium calculation for a plan. Management changed their response to explain the underlying root cause of the error several times. However, PBGC provided no evidence that any analysis was performed to determine the root cause of the error and the extent. Although management knew of the error, it remained uncorrected at year-end and the root cause is still undetermined. This type of error could have a pervasive impact to PBGC's premium calculation for certain plans.

- In April 2013, PBGC's Office of Chief Counsel issued a memo to PBGC's General Counsel and Chief of Negotiations and Restructuring highlighting issues with respect to ERISA IV coverage of Puerto Rico pension plans. Among the recommendations was to withdraw a prior legal opinion regarding Puerto Rico plans' coverage, set standards for PBGC to conclude that a plan was not covered, and to work cooperatively with the Internal Revenue Service to make other coverage determinations. Until noted by the auditors, management did not: 1) disclose this determination to the auditors; 2) consider the legal determination's impact to its premium revenue; and 3) disclose this matter in its fiscal years 2013 and 2014 financial statements. Because of the complexity of coverage issues, PBGC asserts that it cannot identify potentially-impacted plans.

  We observed that the premium income from two Puerto Rico plans had been reversed out of premium revenue based on determinations that neither were covered plans. Management stated, however, that as of September 30, 2014, neither plan had received all premium refunds. This error was not material to the financial statements.

- The design of the control for the reconciliation of the PPS subsidiary ledger to the general ledger is flawed. We found the following reconciliation design deficiencies:

  - The PPS subsidiary balance reported in the reconciliation does not match the underlying details because it included manual activities recorded outside PPS.
  - While management characterizes the aforementioned schedule as reconciliation, it actually represents a calculation of the projected general ledger balance at a point in time. Therefore, the PPS subsidiary ledger could not be reconciled to the general ledger.
  - The reconciliation did not show evidence of a preparer sign-off and supervisory review and approval.

- There is a limitation with the PPS reporting functionality. FOD implemented the new PPS on January 1, 2014, which is used as their premium subsidiary ledger. During our substantive testing at June 30, 2014 and September 30, 2014, we found that PPS functionality is limited because it could not generate a detailed report that displayed the calculated fixed rate and variable rate premium for each pension plan for the period of October 1, 2013 through September 30, 2014.

Recommendations:

- FOD should perform a comprehensive analysis of key data inputs (e.g., participant count, market value, etc) between Form 5500 and the Comprehensive Premium Filing to identify significant variances. In addition, management should develop a risk analysis that focuses on evaluating the underlying causes of the significant variances identified from the comprehensive analysis and assess the potential impact to the completeness assertion for premiums. **(OIG Control # FS-14-15)**

- FOD should perform a period to period (e.g., year to year, quarter to quarter, etc.) fluctuation/variance analysis of plan premium summary level data to identify anomalies, unusual trends, and other critical factors evaluated by management. The underlying cause of the variances should be investigated and documented based on thresholds established by management. **(OIG Control # FS-14-16)**

- FOD should develop a comprehensive list of premium filing scenarios that could impact the premium income accrual calculations. These scenarios should be used to update/refine the PPS system calculation functionality. **(OIG Control # FS-14-17)**

- FOD management should perform periodic inquiries of other Departments and/or Division managers (e.g., General Counsel) within PBGC to obtain relevant information such as status of legal cases and consultation with respect to the appropriate premium refund, and determine impact on the premium revenue calculations and/or financial statement disclosures. These inquires and related responses should be documented and readily available for review by management and/or other key stakeholders such as the OIG and the auditors. **(OIG Control # FS-14-18)**

- FOD management should update their financial statement footnotes disclosures to adequately disclose pertinent events or circumstances that provide useful information and focus user's attention on matters that are most relevant to understanding premium revenue. **(OIG Control # FS-14-19)**

- FOD should develop a procedure to reconcile the PPS subsidiary ledger to general ledger reconciliation. The reconciliation must reflect the cumulative PPS subsidiary balance compared to the general ledger at a point in time (e.g., December 31, March 31, June 30, etc). Any differences should be aggregated by type (e.g., timing differences, manual adjustments) and explained. The support for these differences must be maintained for supervisory and/or external review. In addition, each reconciliation must show evidence of preparer and supervisory review. **(OIG Control # FS-14-20)**

- PBGC should update current procedures and the Premium cycle memo to reflect current control activities and/or practices related to the premium reconciliation process. **(OIG Control # FS-14-21)**

- FOD should update current Premium and Practitioner System reporting functionality to provide a detailed summary fixed and variable rate premium report by plan for each reporting period. This report should be used as the principal support for the PPS balance reported on the PPS subsidiary ledger to general ledger reconciliation. **(OIG Control # FS-14-22)**

B. Lack of controls over the manual processes

The use of manual processes to record financial transactions increases PBGC's susceptibility to erroneous financial reporting. The controls surrounding manual process should compensate for a lack of a fully automated processing environment. PBGC recorded 2,648 manual entries with a total absolute value of approximately $1.756 trillion through June 30, 2014. PBGC did not employ a sequential numbering scheme to assign journal entry numbers. In addition, management did not maintain a journal entry log to ensure the population was complete and that no unauthorized entries were made in the CFS.

Further, PBGC should improve the integrity and access controls of key financial spreadsheets that support the Corporation's financial reporting. PBGC did not have adequate integrity controls to guard against improper modification, access or degradation of key financial spreadsheets. Manual spreadsheets created by various PBGC departments are used extensively by FOD in the financial reporting process. Spreadsheets have inherent control weaknesses, yet the risks were not documented and a mitigation strategy developed. FOD relied on these spreadsheets without establishing baseline integrity and access controls. We identified control deficiencies such as unrestricted file paths, inappropriate administrative accounts, access being granted at the parent folder level, and significant difficulty responding to audit inquiries regarding integrity and access controls. In addition, prior to our request for an inventory of all financial spreadsheets used to record transactions into the CFS, we found that PBGC did not maintain a listing of all key financial reporting spreadsheets.

Moreover, in our examination of PBGC's manual spreadsheet environment, management did not demonstrate that technical access controls are in place to restrict Active Directory account groups to enforce the "principle of least privilege" and protect key financial spreadsheets used in its operations. Our test results identified access controls exceptions related to unauthorized access or access in excess of the level needed to accomplish the specific business tasks. Within numerous spreadsheets that are critical to financial reporting, we found inappropriate access and violations of the need-to-know principal. Though these spreadsheets were created and managed by FOD, Policy, Research and Analysis Department (PRAD), Office of Negotiations & Restructuring (ONR), and BAPD, financial reporting ultimately is the responsibility of the Chief Financial Officer.

Recommendations:

- FOD should develop a sequential numbering scheme to label all entries made by General Accounting Branch (GAB) into CFS. **(OIG Control # FS-14-23)**
- FOD should develop and maintain a log to record and monitor all manual entries entered into CFS by GAB. **(OIG Control # FS-14-24)**
- FOD should develop policies and procedures that will ensure that all journal entries are properly prepared and posted each month. **(OIG Control # FS-14-25)**
- FOD should maintain a complete listing of all key financial spreadsheets. **(OIG Control # FS-14-26)**
- Develop a procedure to update the key financial listing that is provided to the CFO annually. **(OIG Control # FS-14-27)**
- Establish a policy that outlines responsibilities for business owners that create key financial spreadsheets. **(OIG Control # FS-14-28)**
- FOD should conduct a risk assessment to evaluate PBGC's reliance on key financial spreadsheets that support the Corporation's financial reporting. **(OIG Control # FS-14-29)**
- PBGC should develop and implement access and integrity controls to assure the completeness and accuracy of key financial spreadsheets. **(OIG Control # FS-14-30)**
- PBGC should develop and implement procedures that require business owners who prepare key financial spreadsheets to document and provide evidence of their implementation of integrity and access controls. **(OIG Control # FS-14-31)**
- PBGC should develop and implement a process to restrict personnel access to key financial spreadsheets on a "need-to-know" basis. **(OIG Control # FS-14-32)**
- PBGC should develop and implement a process to recertify personnel accounts assigned to network directories holding key financial spreadsheets. **(OIG Control # FS-14-33)**

C. Monitoring Controls over Non-Commingled Assets

PBGC's monitoring process over the valuation of the Non-Commingled Assets (NCAs) is deficient. We found the department responsible for recording plan asset activities performed inadequate reviews of plan asset transactions recorded into the general ledger, processed untimely transfers of non-commingled assets to commingled assets and did not maintain the case file documentation needed to support plan asset transactions. During FY 2014, we examined a sample of 25 trusteed plans. We reviewed the related plan case file for supporting documentation including bank statements, Investment Accounting Branch (IAB) DoPT summaries, PBGC trial balances and other Trust Accounting System (TAS) reports. We calculated a 32% error rate (six sample plans with one exception for each plan and two sample plans with two exceptions for each plan out of 25 sample plans tested) as follows:

- For seven (7) of the twenty five (25) trusteed plans sampled, the net asset values did not agree to supporting documentation within the case file.
- For one (1) of the twenty five (25) trusteed plans sampled, no case file or supporting document was provided for testing.
- For two (2) of the twenty five (25) trusteed plans sampled, the plans were not timely to commingled assets.

Recommendations:

- FOD should review the account balances of the seven (7) identified plans (case #21087700, #22007900, #20291300, #22037300, #22284000, #22321200, and #21951900) to ensure the net asset values are appropriate and make any necessary adjusting entries. Further, IAB should review the account balance of case #4073501 and determine appropriate action for closing out the outstanding balance. **(OIG Control # FS-14-34)**

- FOD should strengthen their internal control procedures by establishing steps to ensure all Trust Accountants (TAs) are recording non-commingled account balances appropriately and consistently. In addition, the procedures should specify a review and/or reconciliation process that should be performed by personnel with sufficient experience and knowledge and in a timely manner to ensure errors are identified and corrected within the same accounting period. **(OIG Control # FS-14-35)**

- FOD should hold training for all TA's once the revised procedures are finalized to ensure proper understanding. **(OIG Control # FS-14-36)**

- Corporate Investment Department should commingle the two (2) plans: Easter Seals Employees – Southwest Ohio (#21087700) and Associated Cleaning Consultants (#20291300). **(OIG Control # FS-14-37)**

- Corporate Investment Department should strengthen their internal control procedures to include a review process of non-commingled plan assets that have been trusteed but not yet transferred to commingle over an extended period of time. These procedures should include specific criteria (i.e. timeframes and asset values) for identifying plan assets that should be considered for transfer. **(OIG Control # FS-14-38)**

5. Present Value of Nonrecoverable Future Financial Assistance

In the future, some multiemployer plans will not be able to meet their benefit obligations of the plan participant. The PV NRFFA represents the estimated nonrecoverable payments PBGC will make to these multiemployer plans. The PV NRFFA balance increased more than 4.4 times, from approximately $10 billion in FY 2013 to approximately $44 billion this fiscal year due mainly to a new classification of one large pension plan moving from Reasonably Possible to Probable. The future multiemployer liability is categorized in three ways, with different disclosure treatment: (1) PBGC records the PV NRFFA in its financial statements for ongoing multiemployer with a projected Date of Insolvency (DOI) within 10 years (probable); (2) financial statement footnote disclosure is made for the Reasonable Possible (DOI is between ten and 20 years); and (3) no disclosure is made for the Remote category (DOI is beyond 20years).

During our PV NRFFA testing as of 9/30/2014, we found a lack of a robust quality control review of the PV NRFFA valuation process. Specifically:

- Inappropriate documentation was used or documentation was misinterpreted to support the valuation. MEPD and ASD relied on insufficient evidence to analyze and compute the liability of one of its largest plan, which represents 45% of the total PV NRFFA liability. For example, ASD used an email from the fund's Chief Financial Officer as the source for the market value of an asset used as input to compute the PV NRFFA liability. Upon our request for the documentation to support the fair market value, ASD obtained a copy of the plan's balance sheet and noted that the balance included a contribution receivable that should not have been included as an input to calculate the PBGC liability. Management subsequently made the adjustment, which increased the PV NRFFA liability by approximately $81 million.

- Input into IPVFB system contained a data entry error. The ASD quality control review process failed to identify an input error made by a preparer. Management subsequently corrected the error, which decreased the PV NRFFA liability by approximately $36 million.

- Misstatements of the expected employer withdrawal liability payments existed in the cash flows projection. Incorrect inputs were entered into IPVFB for the employer withdrawal liability schedules. Additionally, ASD did not obtain the employer withdrawal liability schedules for some plans.

- The most recent data available was not used. ASD did not have a tracking system to send requests to plan trustees for the most recent data for their valuation and to monitor the response. We identified an incorrect exclusion of a due and unpaid employer withdrawal liability payment from the cash flow projection without any evidence that the payment would not be made. Also, ASD did not use the appropriate guaranteed factor to derive the PBGC liability, which generated an understatement of $40 million.

- IPVFB data was missing documentation. ASD did not provide evidence to support the exclusion of employer withdrawal liability payment schedules.

We identified errors in approximately 23% of the sample items tested where the liability calculated for multiemployer plans was misstated. We projected the value of the error to the entire PV NFFA liability of approximately $43 billion at September 30, 2014. Using a

statistically-based sample technique, we estimated a range of approximately $118 million understatement to $157 million overstatement. The point estimate is a $74 million understatement to the approximately $43 billion PV NFFA liability at September 130, 2014.

Recommendations:

- The Actuarial Services Division/BAPD should strengthen its quality control review process over the Present Value of Nonrecoverable Future Financial Assistance to verify that all key data is properly supported and reasonable. **(OIG Control # FS-14-39)**

- The Actuarial Services Division/BAPD should implement the corrections of the errors identified by the auditors during the FY 2014 testing of the Present Value of Nonrecoverable Future Financial Assistance (for samples 17, 22, 27, 33, and 34). **(OIG Control # FS-14-40)**

- The Actuarial Services Division/BAPD should undertake a consolidation and codification of its technical procedures and actuarial practices into a single documentation source for single employer plan valuations. **(OIG Control # FS-14-41)**

- The Actuarial Services Division/BAPD should undertake a consolidation and codification of its technical procedures and actuarial practices into a single documentation source for multiemployer plan valuations. **(OIG Control # FS-14-42)**

- The Actuarial Services Division/BAPD should undertake training of its staff to ensure implementation of the established policy for obtaining up-to-date plan and valuation data for all cases. **(OIG Control # FS-14-43)**

- The Actuarial Services Division/BAPD should implement a tracking system to monitor its request for the most recent data to ensure timely response. **(OIG Control # FS-14-44)**

- The Actuarial Services Division/BAPD should develop a comprehensive policy that describes specific acceptable documentation requirements used to support plan liability valuation. In addition, the policy should include documentation retention requirements. For example, maintenance requirements for old withdrawal liability payment schedules that impact a plan valuation. **(OIG Control # FS-14-45)**

We also found two (2) similar issues of lack of robust quality control review process over the PV NRFFA liability for Probable Small Plan Bulk Reserve (SPBR) and Reasonably Possible SPBR, which understated the PV NRFFA Probable SPBR by approximately $8.4 million and overstated the PV NRFFA Reasonably Possible SPBR by approximately and $55 million. The Office of Negotiations and Restructuring Actuarial Division omitted a small plan terminated during 2009 into its tool for the PV NRFFA Probable SPBR. Further there was a flaw in the calculation of the adjustment factor because NRAD did not update its SPBR tool for the PV NRFFA Reasonably Possible SPBR.

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

***Recommendations*:**

- The Office of Negotiations and Restructuring Actuarial Division should implement a process to monitor the raw data entered into the tool to identify missing plan data and supplement as needed. **(OIG Control # FS-14-46)**

- The Office of Negotiations and Restructuring Actuarial Division should update its Small Plan Bulk Reserve tool to correct the flaws identified by the auditors during the FY 2014 testing. **(OIG Control # FS-14-47)**

- The Office of Negotiations and Restructuring Actuarial Division should promptly correct the two (2) exceptions identified by the auditors during the review performed as of September 30, 2014, which resulted in understatement of multiemployer Probable Small Plan Bulk Reserve (SPBR) and Reasonably Possible SPBR. **(OIG Control # FS-14-48)**

EXHIBIT II

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

Status of Internal Control Report Recommendations

Prior Year Internal Control Report Recommendations Closed During FY 2014:

Recommendation	Date Closed	Original Report Number
FS-07-04	10/06/2014	2008-2/FA-0034-2
FS-07-13	10/06/2014	2008-2/FA-0034-2
FS-07-18	10/03/2014	2008-2/FA-0034-2
FS-08-03M-B	09/18/2014	AUD-2009-2/FA-08-49-2
FS-09-13	10/03/2014	AUD-2010-2/FA-09-64-2
FS-09-19	10/03/2014	AUD-2010-2/FA-09-64-2
FS-11-02	09/18/2014	AUD-2012-2/FA-11-82-2
FS-11-04	10/03/2014	AUD-2012-2/FA-11-82-2
FS-11-05	10/03/2014	AUD-2012-2/FA-11-82-2
FS-11-10	09/11/2014	AUD-2012-2/FA-11-82-2
FS-13-03	09/18/2014	AUD-2014-3/FA-13-93-2
FS-13-04	09/18/2014	AUD-2014-3/FA-13-93-2
FS-13-05	09/18/2014	AUD-2014-3/FA-13-93-2
FS-13-06	09/18/2014	AUD-2014-3/FA-13-93-2

Open Recommendations as of September 30, 2014:

Recommendation	Report
Prior Years'	
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-07-14	2008-2/FA-0034-2
FS-07-17	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-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

EXHIBIT II

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

Recommendation	Report
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-09-20 **	AUD-2010-2/FA-09-64-2
FS-11-03 **	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-11-11	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
FS-13-01 **	AUD-2014-3/FA-13-93-2
FS-13-02	AUD-2014-3/FA-13-93-2
FS-13-07 **	AUD-2014-3/FA-13-93-2
FY Ended September 30, 2014	
FS-14-01	AUD-2015-3/FA-14-101-3
FS-14-02	AUD-2015-3/FA-14-101-3
FS-14-03	AUD-2015-3/FA-14-101-3
FS-14-04	AUD-2015-3/FA-14-101-3
FS-14-05	AUD-2015-3/FA-14-101-3
FS-14-06	AUD-2015-3/FA-14-101-3
FS-14-07	AUD-2015-3/FA-14-101-3
FS-14-08	AUD-2015-3/FA-14-101-3
FS-14-09	AUD-2015-3/FA-14-101-3
FS-14-10	AUD-2015-3/FA-14-101-3
FS-14-11	AUD-2015-3/FA-14-101-3
FS-14-12	AUD-2015-3/FA-14-101-3
FS-14-13	AUD-2015-3/FA-14-101-3
FS-14-14	AUD-2015-3/FA-14-101-3
FS-14-15	AUD-2015-3/FA-14-101-3
FS-14-16	AUD-2015-3/FA-14-101-3
FS-14-17	AUD-2015-3/FA-14-101-3
FS-14-18	AUD-2015-3/FA-14-101-3
FS-14-19	AUD-2015-3/FA-14-101-3
FS-14-20	AUD-2015-3/FA-14-101-3
FS-14-21	AUD-2015-3/FA-14-101-3
FS-14-22	AUD-2015-3/FA-14-101-3
FS-14-23	AUD-2015-3/FA-14-101-3
FS-14-24	AUD-2015-3/FA-14-101-3

EXHIBIT II

Pension Benefit Guaranty Corporation
Supplemental Report on Internal Control
Fiscal Year 2014

Recommendation	Report
FS-14-25	AUD-2015-3/FA-14-101-3
FS-14-26	AUD-2015-3/FA-14-101-3
FS-14-27	AUD-2015-3/FA-14-101-3
FS-14-28	AUD-2015-3/FA-14-101-3
FS-14-29	AUD-2015-3/FA-14-101-3
FS-14-30	AUD-2015-3/FA-14-101-3
FS-14-31	AUD-2015-3/FA-14-101-3
FS-14-32	AUD-2015-3/FA-14-101-3
FS-14-33	AUD-2015-3/FA-14-101-3
FS-14-34	AUD-2015-3/FA-14-101-3
FS-14-35	AUD-2015-3/FA-14-101-3
FS-14-36	AUD-2015-3/FA-14-101-3
FS-14-37	AUD-2015-3/FA-14-101-3
FS-14-38	AUD-2015-3/FA-14-101-3
FS-14-39	AUD-2015-3/FA-14-101-3
FS-14-40	AUD-2015-3/FA-14-101-3
FS-14-41	AUD-2015-3/FA-14-101-3
FS-14-42	AUD-2015-3/FA-14-101-3
FS-14-43	AUD-2015-3/FA-14-101-3
FS-14-44	AUD-2015-3/FA-14-101-3
FS-14-45	AUD-2015-3/FA-14-101-3
FS-14-46	AUD-2015-3/FA-14-101-3
FS-14-47	AUD-2015-3/FA-14-101-3
FS-14-48	AUD-2015-3/FA-14-101-3

* The dates have been revised one or more times by management.

** PBGC has not established a revised completion date.

Report on Internal Controls Related to the
Pension Benefit Guaranty Corporation's
Fiscal Year 2014 and 2013 Financial Statements

Audit Report AUD-2015-3 / FA-14-101-3

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 10, 2014

To: Deborah Stover-Springer
Acting Inspector General

From: Alice C. Maroni
Acting Director

Subject: Response to Draft FY 2014 Internal Control Report

Thank you for the opportunity to comment on the draft FY 2014 internal control report. We agree with most of the findings and recommendations in this year's report and have provided responses to each of the new recommendations in the attachment. The attachment to this memorandum essentially summarizes the details provided to your office in response to the Notices of Findings and Recommendations and gives estimated completion dates where established.

With respect to the agreed-upon recommendations from prior years, we continue to make noteworthy progress. We are especially pleased to note that the significant deficiency regarding Integrated Financial Management Systems has now been addressed. We also appreciate your acknowledgement in the draft report of the other progress made over the past year. 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 on each of the past recommendations.

Again, we are pleased that the report recognizes the corrective actions made in benefits administration, including the improvements to the Benefits Administration and Payment Department operations. We also appreciate the acknowledged improvements being made in addressing IT security through better management of the design, implementation, and

operational effectiveness of our controls. We are committed to continued advances in both BAPD operations and IT security.

We look forward to meeting with your office on any recommendations that may need resolution. 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 your office throughout FY 2015 to make PBGC an even better agency in service to the millions of Americans who depend on us for their pension security.

Attachment

cc:

Edgar Bennett
Patricia Kelly
Cathleen Kronopolus
Ann Orr
Michael Rae
Sanford Rich
Judith Starr
Martin O. Boehm
Theodore J. Winter

Attachment

Note: To facilitate communication, we have provided provisional numbers parenthetically to the OIG recommendations, based upon their sequence within the draft report.

BAPD Management and Oversight

OIG Recommendation: Promptly correct errors in its calculations and data entries identified by the auditors during FY 2014. (OIG Control # FS-14-XX) (14-01)

PBGC Response: Management agrees. BAPD will promptly correct errors in its calculations, as noted in our responses to the Notices of Findings and Recommendations.

OIG Recommendation: PBGC should perform an analysis to identify risks associated with a lack of documentation to support all participants' benefit calculations and assess the impact to the calculations and related liability. (OIG Control # FS-14-XX) (14-02)

PBGC Response: Management agrees. This work is related to the risk assessment mentioned in response to NFR 14-02. We look forward to further discussions regarding the documentation issue.

OIG Recommendation: Upon completion of analysis, PBGC should develop a policy to finalize management's position on the financial impact of the lack of documentation issue and any actions that will be taken to address this systemic issue. The policy should also document any residual risk that it may elect to accept. (OIG Control # FS-14-XX) (14-03)

PBGC Response: Management agrees. Upon completion of the risk assessment, management will develop an approach to address the historic documentation issue and specify corrective actions to minimize occurrences in future case processing. BAPD will also document any risks that BAPD decides to accept.

OIG Recommendation: Develop and document a risk assessment of the BAPD's entire operations. The risk assessment should include the identification of all the root causes of the issues identified by the auditors and ASD. PBGC should monitor the implemented corrective actions. The materiality thresholds used should be reasonable. (OIG Control # FS-14-XX) (14-04)

PBGC Response: Management agrees. BAPD will develop and document a risk assessment of its operations that have a direct impact on PVFB liabilities and implement appropriate corrective actions.

OIG Recommendation: Review known cases of miscalculation of the Retirement Service Credit Fraction and determine if plan participants are receiving incorrect benefits. (OIG Control # FS-14-XX) (14-05)

PBGC Response: Management agrees. BAPD will review the Software Close-out Checklist to determine whether additional enhancements are needed to ensure that all documentation needed to support the calculation of Termination Benefits is stored in Archive.

OIG Recommendation: Expand modernization efforts to Spectrum and the Integrated Present Value of Future Benefits (IPVFB) systems to:

1. Value the actual popup benefit for Joint and Survivor Popup annuity forms.

2. Value non-level and surviving spouse benefits without the need for supplemental tables. (OIG Control # FS-14-XX) (14-06)

PBGC Response: Management agrees. Management will work on developing solutions to address both of these issues during Phase 2 of the Spectrum and IPVFB modernization project.

OIG Recommendation: Enhance procedures for computing 4022(c) benefits and document those procedures in the Actuarial Technical Manual. (OIG Control # FS-14-XX) (14-07)

PBGC Response: Management disagrees. As noted in management's response to the first NFR, we already have procedures to address this sort of situation. We will be happy to discuss this with the auditors further, to ensure a common understanding.

Entity-wide Security Program Planning and Management

There were no new recommendations in the internal control report for FY 2014.

Access Controls and Configuration Management

OIG Recommendation: Update and document the security event categorization procedures and decision process to better define the thresholds where security events are categorized as suspicious and are recorded in a ticketing system as an incident for escalation and further analysis. (OIG Control # FS-14-XX) (14-08)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Establish a periodic review (at least quarterly) process for contractor's compliance, including the execution of PBGC's security event categorization procedures and

decision process, review of IDS logs, and other continuous monitoring activity. (OIG Control # FS-14-XX) (14-09)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Ensure that security incidents are documented, investigated, reported to federal management, and corrective actions implemented to remediate security vulnerabilities. (OIG Control # FS-14-XX) (14-10)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Develop factors to prioritize security incidents, such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity, and availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident). (OIG Control # FS-14-XX) (14-11)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk. (OIG Control # FS-14-XX) (14-12)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Develop and implement controls to enhance PBGC's ability to identify inappropriate or unusual activity, integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information. (OIG Control # FS-14-XX) (14-13)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

OIG Recommendation: Review, update, and approve Directive IM 10-3, Protecting Sensitive Information. (OIG Control # FS-14-XX) (14-14)

PBGC Response: This represents a prior recommendation to which management agreed last year in response to the FISMA report.

Financial Reporting

OIG Recommendation: FOD should perform a comprehensive analysis of key data inputs (e.g., participant count, market value, etc) between Form 5500 and the Comprehensive Premium Filing to identify significant variances. In addition, management should develop a risk analysis that focuses on evaluating the underlying causes of the significant variances identified from the comprehensive analysis and assess the potential impact to the completeness assertion for premiums. (OIG Control # FS-14-XX) (14-15)

PBGC Response: Management agrees. Management anticipates focusing on the largest 10 percent of plans with data differences in the first year, pursuing additional layers in subsequent years. Assuming timely resolution of the issues surrounding the underlying supporting information, management's expected target completion date is December 31, 2015.

OIG Recommendation: FOD should perform a period to period (e.g., year to year, quarter to quarter, etc.) fluctuation/variance analysis of plan premium summary level data to identify anomalies, unusual trends, and other critical factors evaluated by management. The underlying cause of the variances should be investigated and documented based on thresholds established by management. (OIG Control # FS-14-XX) (14-16)

PBGC Response: Management agrees. The estimated completion date is June 30, 2015.

OIG Recommendation: FOD should develop a comprehensive list of premium filing scenarios that could impact the premium income accrual calculations. These scenarios should be used to update/refine the PPS system calculation functionality. (OIG Control # FS-14-XX) (14-17)

PBGC Response: Management agrees. The estimated completion date is June 30, 2015.

OIG Recommendation: FOD management should perform periodic inquiries of other Departments and/or Division managers (e.g., General Counsel) within PBGC to obtain relevant information such as status of legal cases and consultation with respect to the appropriate premium refund, and determine impact on the premium revenue calculations and/or financial statement disclosures. These inquires and related responses should be documented and readily available for review by management and/or other key stakeholders such as the OIG and the auditors. (OIG Control # FS-14-XX) (14-18)

PBGC Response: Management agrees. The estimated completion date is June 30, 2015.

OIG Recommendation: FOD management should update their financial statement footnotes disclosures to adequately disclose pertinent events or circumstances that provide useful information and focus user's attention on matters that are most relevant to understanding premium revenue. (OIG Control # FS-14-XX) (14-19)

PBGC Response: Management agrees. Management has already done so for the FY 2014 year-end financial statements and will do so going forward.

OIG Recommendation: FOD should develop a procedure to reconcile the Premium and Practitioner System (PPS) subsidiary ledger to general ledger reconciliation. The reconciliation must reflect the cumulative PPS subsidiary balance compared to the general ledger at a point in time (e.g., December 31, March 31, June 30, etc). Any differences should be aggregated by type (e.g., timing differences, manual adjustments) and explained. The support for these differences must be maintained for supervisory and/or external review. In addition, each reconciliation must show evidence of preparer and supervisory review. (OIG Control # FS-14-XX) (14-20)

PBGC Response: Management agrees. Management's estimated completion date is July 31, 2015, in order to include the June 30, 2015, year-to-date reconciliation.

OIG Recommendation: PBGC should update current procedures and the Premium cycle memo to reflect current control activities and/or practices related to the premium reconciliation process. (OIG Control # FS-14-XX) (14-21)

PBGC Response: Management agrees. The estimated completion date for this work is March 31, 2015.

OIG Recommendation: FOD should update current Premium and Practitioner System reporting functionality to provide a detailed summary fixed and variable rate premium report by plan for each reporting period. This report should be used as the principal support for the PPS balance reported on the PPS subsidiary ledger to general ledger reconciliation. (OIG Control # FS-14-XX) (14-22)

PBGC Response: Management agrees. Management has previously provided reports for the FY 2014 second, third, and fourth quarters and will continue to do so moving forward.

OIG Recommendation: FOD should develop a sequential numbering scheme to label all entries made by General Accounting Branch (GAB) into Consolidated Financial System (CFS). (OIG Control # FS-14-XX) (14-23)

PBGC Response: Management agrees. FOD management would anticipate that the manual journal entries Standard Operating Procedure and the manual journal entry log provided to the auditors and implemented on September 19, 2014 would fully address these three related recommendations.

OIG Recommendation: FOD should develop and maintain a log to record and monitor all manual entries entered into Consolidated Financial System (CFS) by General Accounting Branch (GAB). (OIG Control # FS-14-XX) (14-24)

PBGC Response: Management agrees. See response to 14-23, above.

OIG Recommendation: FOD should develop policies and procedures that will ensure that all journal entries are properly prepared and posted each month. (OIG Control # FS-14-XX) (14-25)

PBGC Response: Management agrees. See response to 14-23, above.

OIG Recommendation: FOD should maintain a complete listing of all key financial spreadsheets. (OIG Control # FS-14-XX) (14-26)

PBGC Response: Management agrees. PBGC will conduct a review, update, and maintain our listing of key financial spreadsheets. We expect to complete the work on this recommendation by January 30, 2015.

OIG Recommendation: Develop a procedure to update the key financial listing that is provided to the CFO annually. (OIG Control # FS-14-XX) (14-27)

PBGC Response: Management agrees. PBGC will document our procedure to update our listing of key financial spreadsheets, including a procedure to report the list and any list updates to the CFO on an annual basis. We expect to complete the work on this recommendation by January 30, 2015.

OIG Recommendation: Establish a policy that outlines responsibilities for business owners that create key financial spreadsheets. (OIG Control # FS-14-XX) (14-28)

PBGC Response: Management agrees. PBGC will document our procedure to update our listing of key financial spreadsheets, including adoption of the AICPA best practices. We expect to complete the work on this recommendation by January 30, 2015.

OIG Recommendation: FOD should conduct a risk assessment to evaluate PBGC's reliance on key financial spreadsheets that support the Corporation's financial reporting. (OIG Control # FS-14-XX) (14-29)

PBGC Response: Management agrees. PBGC will conduct and document a risk assessment to evaluate financial reporting reliance on key financial spreadsheets. We expect to complete the work on this recommendation by February 27, 2015.

OIG Recommendation: PBCG should develop and implement access and integrity controls to assure the completeness and accuracy of key financial spreadsheets. (OIG Control # FS-14-XX) (14-30)

PBGC Response: Management agrees. PBGC's Contracts and Controls Review Department (CCRD) will work with relevant departments to develop and implement controls over key financial spreadsheets, including providing training opportunities for employees. We expect to complete the work on this recommendation by June 30, 2015.

OIG Recommendation: PBGC should develop and implement procedures that require business owners who prepare key financial spreadsheets to document and provide evidence of their implementation of integrity and access controls. (OIG Control # FS-14-XX) (14-31)

PBGC Response: Management agrees. CCRD will work with the germane departments to document that controls over key financial spreadsheets are in place. We expect to complete the work on this recommendation by June 30, 2015.

OIG Recommendation: PBCG should develop and implement a process to restrict personnel access to key financial spreadsheets on a "need-to-know" basis. (OIG Control # FS-14-XX) (14-32)

PBGC Response: Management agrees. We will leverage our existing processes for restricting personnel access to key financial spreadsheets on a "need-to-know" basis. Our planned completion date for securing folder enhancements across PBGC financial spreadsheets used by FOD, ONR, BAPD, and PRAD is February 27, 2015.

OIG Recommendation: PBCG should develop and implement a process to recertify personnel accounts assigned to network directories holding key financial spreadsheets. (OIG Control # FS-14-XX) (14-33)

PBGC Response: Management agrees. PBGC will include the recertification of personnel accounts assigned to network directories holding key financial spreadsheet within its Annual Account Recertification Process. Our planned completion date for access control recertifications is June 30, 2015.

OIG Recommendation: FOD should review the account balances of the seven (7) identified plans (case #21087700, #22007900, #20291300, #22037300, #22284000, #22321200, and #21951900) to ensure the net asset values are appropriate and make any necessary adjusting entries. Further, IAB should review the account balance of case #4073501 and determine appropriate action for closing out the outstanding balance. (OIG Control # FS-14-XX) (14-34)

PBGC Response: Management agrees. As of October 9, 2014, IAB reviewed the seven identified plans and made all related adjusting entries. In addition, IAB reviewed the account balance of the Campbell's Furniture, Inc. plan and closed out the outstanding balance.

OIG Recommendation: FOD should strengthen their internal control procedures by establishing steps to ensure all Trust Accountants (TAs) are recording non-commingled account balances appropriately and consistently. In addition, the procedures should specify a review and/or reconciliation process that should be performed by personnel with sufficient experience and knowledge and in a timely manner to ensure errors are identified and corrected within the same accounting period. (OIG Control # FS-14-XX) (14-35)

PBGC Response: Management agrees. PBGC sees significant value in the two-tiered approach discussed in response to the NFR, focusing our limited resources on those $5 million-plus plans that have potentially larger impact (though not necessarily material impact) on the non-commingled asset balances.

OIG Recommendation: FOD should hold training for all TA's once the revised procedures are finalized to ensure proper understanding. (OIG Control # FS-14-XX) (14-36)

PBGC Response: Management agrees. IAB scheduled Trust Accounting training for the revised procedures beginning in November 2014.

OIG Recommendation: Corporate Investment Department should commingle the two (2) plans: Easter Seals Employees – Southwest Ohio (#21087700) and Associated Cleaning Consultants (#20291300). (OIG Control # FS-14-XX) (14-37)

PBGC Response: Management agrees. Management has already addressed this as noted in the response to the NFR.

OIG Recommendation: Corporate Investment Department should strengthen their internal control procedures to include a review process of non-commingled plan assets that have been trusteed but not yet transferred to commingled over an extended period of time. These procedures should include specific criteria (i.e. timeframes and asset values) for identifying plan assets that should be considered for transfer. (OIG Control # FS-14-XX) (14-38)

PBGC Response: Management agrees. Management has already begun work on this recommendation.

Present Value of Nonrecoverable Future Financial Assistance (PV NRFFA)

OIG Recommendation: The Actuarial Services Division/BAPD should strengthen its quality control review process over the Present Value of Nonrecoverable Future Financial Assistance to verify that all key data is properly supported and reasonable. (OIG Control # FS-14-XX) (14-39)

PBGC Response: Management agrees. ASD will strengthen the quality control process for the determination of the Present Value of Nonrecoverable Future Financial Assistance. ASD will evaluate and implement new methods of verifying and ensuring that all key data is properly supported and reasonable.

OIG Recommendation: The Actuarial Services Division/BAPD should implement the corrections of the errors identified by the auditors during the FY 2014 testing of the Present Value of Nonrecoverable Future Financial Assistance (for samples 17, 22, 27, 33, and 34). (OIG Control # FS-14-XX) (14-40)

PBGC Response: Management agrees. ASD will correct the errors identified (samples 17, 22, 27, 33, and 34).

OIG Recommendation: The Actuarial Services Division/BAPD should undertake a consolidation and codification of its technical procedures and actuarial practices into a single documentation source. This should include single employer and multiemployer plan valuations. (OIG Control # FS-14-XX) (14-41)

PBGC Response: Management agrees. ASD will consolidate and codify applicable technical procedures and actuarial practices for ASD's valuation of PBGC's single employer and multiemployer programs. This consolidation/codification will be done in conjunction with the IPVFB modernization. In FY14, we started Phase 1 of the IPVFB modernization effort. Phase 2 is expected to begin in FY15. Technical procedures and actuarial practices will be documented during the modernization.

OIG Recommendation: The Actuarial Services Division/BAPD should undertake training of its staff to ensure implementation of the established policy for obtaining up-to-date plan and valuation data for all cases. Create a follow-up system to remind plans when requested data is not provided. (OIG Control # FS-14-XX) (14-42)

PBGC Response: Management agrees. ASD will ensure implementation of ASD's established policy for obtaining updated plan and valuation data for all cases. ASD will create and implement a tracking system for monitoring requests for updated data and for following up when requested data is not provided. ASD will also provide training for ASD multiemployer plan staff on the policy and the tracking system to ensure implementation of the policy.

OIG Recommendation: The Actuarial Services Division/BAPD should develop a comprehensive policy that describes specific acceptable documentation requirements used to support plan liability valuation. In addition, the policy should include documentation retention requirements. For example, maintenance requirements for old withdrawal liability payment schedules that impact a plan valuation. (OIG Control # FS-14-XX) (14-43)

PBGC Response: Management agrees. ASD will develop a policy that documents acceptable documentation requirements to support ASD's valuation of multiemployer plan liabilities. The policy will include document retention requirements, including maintenance requirements for prior withdrawal liability payment schedules that may impact future plan valuations.

OIG Recommendation: The Actuarial Services Division/BAPD should implement a tracking system to monitor its request for the most recent data to ensure timely response. (OIG Control # FS-14-XX) (14-44)

PBGC Response: Management agrees. ASD will create and implement a tracking system for monitoring requests for updated data and for following up when requested data is not provided.

OIG Recommendation: The Office of Negotiations and Restructuring Actuarial Division should implement a process to monitor the raw data entered into the tool to identify missing plan data and supplement as needed. (OIG Control # FS-14-XX) (14-45)

PBGC Response: Management agrees. Management will address this in the Small Plan Bulk Reserve process for FY 2015.

OIG Recommendation: The Office of Negotiations and Restructuring Actuarial Division should update its Small Plan Bulk Reserve tool to correct the flaws identified by the auditors during the FY 2014 testing. (OIG Control # FS-14-XX) (14-46)

PBGC Response: Management agrees. Management will address this in the Small Plan Bulk Reserve process for FY 2015.

OIG Recommendation: The Office of Negotiations and Restructuring Actuarial Division should promptly correct the two (2) exceptions identified by the auditors during the review performed as of September 30, 2014, which resulted in understatement of multiemployer Probable Small Plan Bulk Reserve (SPBR) and Reasonably Possible SPBR. (OIG Control # FS-14-XX) (14-47)

PBGC Response: Management agrees with the finding and has already responded to this recommendation in the response to NFR 14-22.

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