Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation Report

Fiscal Year 2014 Federal Information Security Management Act Final Report

May 6, 2015

EVAL 2015-9/FA-14-101-7

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

May 6, 2015

TO: Alice Maroni
Chief Management Officer

Robert Scherer
Chief Information Officer

FROM: Rashmi Bartlett
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2014 Federal Information Security Management Act Independent Evaluation Report (EVAL-2015-9/FA-14-101-7)

I am pleased to transmit the final fiscal year (FY) 2014 Federal Information Security Management Act (FISMA) report, detailing the results of our review of the Pension Benefit Guaranty Corporation (PBGC) information security program.

As prescribed by FISMA, the PBGC Inspector General is required to conduct annual evaluations of the PBGC security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this evaluation. CliftonLarsonAllen LLP, on behalf of the PBGC OIG, completed the OMB-required responses that we then submitted to OMB. This evaluation report provides additional information on the results of our review of the PBGC information security program.

PBGC agreed with all recommendations in this report. Information Technology (IT) security remains a challenge for PBGC management. Long-standing security weaknesses are unresolved. PBGC's corrective action plan continues to push out timelines for resolution. Some recommendations to correct these weaknesses date back to FY 2005 and are not scheduled for completion until FY 2018. Although remediation has been slow we observed some improvements in PBGC's 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.

We appreciate the overall cooperation CliftonLarsonAllen and OIG received during the audit.

Attachment

cc:
Edgar Bennett
Patricia Kelly
Cathleen Kronopolus
Ann Orr
Michael Rae
Sandy Rich
Judith Starr
Tim Hurr
Joshua Kossoy
Marty Boehm

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Deborah Stover-Springer
Acting Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, N.W.
Washington, DC 20005-4026

Dear Ms. Stover-Springer:

We are pleased to provide the Fiscal Year (FY) 2014 Federal Information Security Management Act (FISMA) Independent Evaluation Report, detailing the results of our review of the Pension Benefit Guaranty Corporation (PBGC) information security program.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FISMA requires Inspectors General (IG) to conduct annual evaluations of their agency's security programs and practices, and to report to Office of Management and Budget (OMB) the results of their evaluations. OMB Memorandum M-15-01, *"Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*" provides instructions for completing the FISMA evaluation. Evaluations conducted by Offices of Inspector General (OIG) are intended to independently assess whether the agencies are applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions.

CliftonLarsonAllen LLP completed the required FISMA questionnaire on behalf of the PBGC OIG. The OIG then reviewed, approved, and submitted the responses to OMB on November 14, 2014. This evaluation report provides additional information on the results of our review of the PBGC information security program.

In preparing required responses on behalf of the OIG, we coordinated with PBGC management and appreciate their cooperation in this effort. PBGC management has provided us with a response (dated May 1, 2015) to the draft FISMA 2014 Independent Evaluation Report.

The projection of any conclusions, based on our findings, to future periods is subject to the risk that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

CliftonLarsonAllen LLP

Calverton, Maryland
May 1, 2015

TABLE OF CONTENTS

Page

I. EXECUTIVE SUMMARY

The Federal Information Security Management Act (FISMA) requires agencies to adopt a risk-based, life cycle approach to improve computer security that includes annual security program reviews, independent evaluations by the Inspector General (IG), and reporting to the Office of Management and Budget (OMB) and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

Information Technology (IT) security continues to be a challenge for Pension Benefit Guaranty Corporation (PBGC) management. Long-standing security weaknesses remain unresolved. PBGC's corrective action plan continues to push out timelines for resolution. Some recommendations to correct these weaknesses date back to fiscal year (FY) 2005 and are not scheduled for completion until FY 2018. Our audit also uncovered new weaknesses in PBGC's IT security, including:

- A new system was introduced, the PBGC Connect system (i.e. SharePoint), does not have a coherent and actionable plan for protecting Personally Identifiable Information (PII).
- PBGC has not established and implemented an entity-wide information security continuous monitoring (ISCM) strategy and program. The ISCM is required by OMB Memorandum 14-03 for agencies to enhance the security of federal information and information systems. The ISCM will assist PBGC in the active and consistent maintenance of ongoing awareness of its information security, vulnerabilities, and threats to support organizational risk management decisions.
- PBGC IT security personnel do not have the security clearance necessary to have timely access to top secret information needed for prompt security assessment and management.

The safeguarding of PBGC's systems and data is essential for protecting PBGC's operations and mission. The Office of Inspector General (OIG) and others have consistently identified serious internal control vulnerabilities and systemic security control weaknesses in the IT environment over the last decade.

We are reporting nine (9) FISMA findings with thirty-three (33) recommendations for FY 2014 based on the results of our FY 2014 independent evaluation. In addition to those in this report, there were nine (9) FISMA-related findings with thirty-two (32) recommendations reported in the Corporation's FY 2014 internal control report based on our FY 2014 financial statements audit work. There is no overlap in the findings and recommendations in the two reports. Based on the nature of the issues identified and the continued existence of unremediated recommendations, we concluded that PBGC does not have an effective information security program.

II. BACKGROUND

The PBGC protects the pensions of approximately 41 million workers and retirees in more than 24 thousand private defined benefit pension plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined benefit pension plans in the United States. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of IT. Internal controls are essential to ensure the confidentiality, integrity, and availability of critical data while reducing the risk of errors, fraud, and other illegal acts.

PBGC has become increasingly dependent on computerized information systems to execute its operations and to process, maintain, and report essential information. As a result, the reliability of computerized data and of the systems that process, maintain, and report this data is a major priority for PBGC. While the increase in computer interconnectivity has changed the way the government does business, it has also increased the risk of loss and misuse of information by unauthorized or malicious users. Protecting information systems continues to be one of the most important challenges facing government organizations today.

Through FISMA, the U.S. Congress showed its intention to enhance the management and promotion of electronic government services and processes. Its goals are to achieve more efficient government performance, increase access to government information, and increase citizen participation in government. FISMA also provides a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

The Federal Information Security Modernization Act of 2014 was signed on December 18, 2014, to update FISMA (E-Gov. 2002) after the FY 2014 audit period. The Act extends more authority to Department of Homeland Security (DHS) to administer the FISMA; OMB retains policy/procedure authority; DHS can issue "binding operational directives" (compulsory for agencies); and coordinates with National Institute of Standards and Technology (NIST) to avoid conflicts. The Act also modifies required reporting to Congress (less policy, more threat and incident-oriented). It increases focus on detecting, reporting, and responding to security incidents; "confirmed" breach notification to Congress (7 days). Within one year, OMB will revise Circular A-130, *Management of Federal Information Resources,* to eliminate "wasteful/inefficient" reporting requirements.

PBGC operates an open and distributed computing environment to facilitate collaboration and knowledge sharing, and support its mission of protecting the pensions of over 41 million workers and retirees. It faces the challenging task of maintaining this environment, while protecting its critical information assets against malicious use and intrusion.

The PBGC OIG contracted with CliftonLarsonAllen LLP to conduct PBGC's FY 2014 FISMA Independent Evaluation. We performed this evaluation in conjunction with our review of information security controls required as part of the annual financial statement audit.

III. OBJECTIVES

The purpose of this evaluation was to assess the effectiveness of PBGC's information security program and practices and to determine compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

IV. SCOPE & METHODOLOGY

To perform our review of PBGC's security program, we followed a work plan based on the following guidance:

- NIST Special Publication 800-53 Revision 4 *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* for certification and accreditation controls.

- NIST Special Publication 800-53A*, Guide for Assessing the Security Controls in Federal Information Systems,* for the assessment of security control effectiveness.
- Government Accountability Office (GAO)'s *Federal Information System Controls Audit Manual* (FISCAM: GAO-09-232G), for the information technology audit methodology.

The combination of these methodologies allowed us to meet the requirements of both FISMA and the Chief Financial Officer's Act.

Our procedures included internal and external security reviews of PBGC's IT infrastructure; reviewing agency plans of action and milestones (POA&Ms); and evaluating the following subset of PBGC's systems:

- Consolidated Financial System (CFS)
- Trust Accounting System (TAS)
- PBGC Connect (Share Point)
- Premium & Practitioner System (PPS)
- Pension and Lump Sum System (PLUS)

We performed procedures to test (1) PBGC's implementation of an entity-wide security plan, and (2) operational and technical controls specific to each application such as service continuity, logical access, and change controls. We also performed targeted tests of controls over financial and business process applications. We performed our review from April 4, 2014 to September 30, 2014, at PBGC's headquarters in Washington, DC. We also performed a security assessment of the PLUS application in July 2014 at State Street Corporation in Quincy, Massachusetts.

This independent evaluation was prepared based on information available as of September 30, 2014.

V. SUMMARY OF CURRENT YEAR TESTING

Title III of the E-Government Act (Public Law No. 104-347), also called the FISMA, requires agencies to adopt a risk-based, life cycle approach to improving computer security that includes annual security program reviews, independent evaluations by the IG, and reporting to the OMB and the Congress. It also codifies existing policies and security responsibilities outlined in the Computer Security Act of 1987 and the Clinger Cohen Act of 1996.

IT security continues to be a challenge for PBGC management. Long-standing security weaknesses remain unresolved. PBGC's corrective action plan continues to push out timelines for resolution, some of which are not scheduled for completion until FY 2018.

In this year's audit, we identified nine new weaknesses that included system design and implementation that failed to adequately protect PII. PBGC introduced a new system, PBGC Connect system (i.e. SharePoint), that did not have a coherent and actionable plan for protecting PII. PBGC has not established and implemented OMB Memorandum 14-03 (M-14-03), *Enhancing the Security of Federal Information and Information Systems*. M-14-03 required federal agencies to establish and implement an entity-wide ISCM strategy and program by February 28, 2014. Currently, PBGC IT security personnel do not have timely access to top secret information. Security clearance is required to be briefed on security events, trends and strategies.

Over the last decade, serious internal control vulnerabilities and systemic security control weaknesses have been consistently identified by the OIG and others. As a result, we issued a total of 62 FISMA and FISMA-related recommendations: 30 recommendations are in this report (FY 2014 independent FISMA evaluation); and 32 recommendations were reported in the Corporation's FY 2014 internal control report, noted in Section VII.

Our review of IT controls covered general and selected business process application controls. General controls are the structure, policies, and procedures that apply to an entity's overall computer systems. They include entity-wide security management, access controls, configuration management, segregation of duties and contingency planning controls. Business process application controls are those controls over the confidentiality, integrity and availability of transactions and data during application processing.

PBGC continued to remediate conditions that contribute to the previously identified deficiencies with its internal controls noted in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2013 and 2012 Financial Statement Audit* and other reports. We observed some improvements in PBGC's 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 Corporation 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.

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 long standing security control weaknesses in the following areas that have been reported for many years. Some recommendations to correct these weaknesses date back to FY 2005 and remediation is not planned until FY 2018.

1. Entity-wide Security Program Planning and Management

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 controls continued to be changed, creating an unstable environment to effectively implement the controls. These common security controls provide the foundation for the effectiveness of enterprise-wide system security operations. Weaknesses noted in PBGC's implementation of common controls include the following:

- 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.
- After the consolidation, the Corporation was considering adding 67 new controls to the set of common controls.
- 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 55 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 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.

2. 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 it believed supported 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.

PBGC's documentation of corrective action taken and evidence to support closure of a recommendation has been weak. Quality controls are inadequate to ensure PBGC can demonstrate remediation of security weaknesses before recommending closure to the OIG. PBGC may have the wrong impression that security weaknesses have been addressed, even though they provided to the OIG incomplete or inaccurate information as evidence for closure of recommendation.

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 critical systems 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.

The financial internal control findings related to entity-wide security program planning and management, access controls and configuration management were reported in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2014 and 2013 Financial Statements Audit* (AUD-2015-3 /FA-14-101-3)[1] issued on November 14, 2014. As a result of our findings, we made recommendations to correct the deficiencies. A table summarizing these findings is in Section VII of this report.

In addition, we are reporting deficiencies in the following FISMA areas for FY 2014:

1. Information Technology Controls for The Protection of Privacy;
2. Plan of Action and Milestones (POA&M);
3. Shared Accounts;
4. Information Security Continuous Monitoring (ISCM) Program;
5. PBGC Security Clearance – High Risk Designation
6. PBGC Reinvestigation
7. PBGC IP Address Inventory
8. Application Specific General Controls; and
9. Review of Interconnection Security Agreements.

In addition, our audit also found deficiencies specifically related to responses required by OMB M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (October 3, 2014) which are included in this report. These findings and recommendations, not previously reported, are as follows.

[1] http://oig.pbgc.gov/pdfs/FA-14-101-3.pdf

VI. FINDINGS AND RECOMMENDATIONS

1. Information Technology Controls for The Protection of Privacy

Issues regarding the protection of sensitive information continue to exist from previous years. PBGC has not implemented controls to protect all PII in its development environment, which does not have the same level of security controls as its production systems. In FY 2013, PBGC selected a data masking solution to address PII data in non-production environments. PBGC Management indicated they plan to design and acquire the data masking solution in FY 2014.

Recommendations:

- Remove PII from the development environment. **(OIG Control Number FISMA-11-02)**

  PBGC's Scheduled Completion Date: 8/30/2015

PBGC's Site Collection Owners did not document or establish a policy governing the use of PBGC Connect sites (i.e. SharePoint). At the present time, about 15-20% of business organizations are using SharePoint. The Site Collection Owners are accountable for all of the sites, content, and administrative settings within their assigned site collection(s). The Site Collection Owners have not developed policy for site users.

The scope of the *PBGC Connect Governance Plan* pertains to the technologies and three governance segments: information management, technology management and application management. The *PBGC Connect Governance Plan* does not define business user practices for PBGC Connect.

PBGC implemented PBGC Connect, also known as SharePoint, as an enterprise-wide content management tool to manage unstructured data. Unstructured data involves many of the most common documents and record formats. Items such as Microsoft Word documents, Excel spreadsheets, or PowerPoint presentations are common examples of unstructured data. Unstructured data from various sources are to migrate to PBGC Connect, such as documents from shared network drives and PBGC's Intranet.

Currently, the type of data stored on PBGC Connect was up to the discretion of each business unit. There were no controls in place to restrict business units from bypassing application business rules and storing structured, application-derived data inappropriately in PBGC Connect. Structured data describes the information stored in databases or applications and that has a very well-defined structure. Databases and applications have strong business process controls, including input validation controls, integrity controls and security controls. Controls governing application data will not be effective outside the application, which might adversely impact decision making and business processes.

The *PBGC Connect Governance Plan* states that business users can store PII, under designated Controlled Unclassified Information (CUI) sites in PBGC Connect. PII is not permitted in sites not designated as CUI. Currently PBGC Connect Administrators monitor for PII by performing manual and daily searches to identify any PII that has been uploaded to PBGC Connect without the proper access restrictions. When the daily PII searches result in the detection of unprotected PII, an e-mail is sent to the site owner and author notifying them that sensitive information has been detected and should be removed or redacted. Until the PII is removed by the site owner or author, it is available to all PBGC Connect users. A draft

procedure, *SharePoint Fast Search & PII Data Daily Check*, is available to guide administrators through the daily search process; however, there was no formal procedure or defined timeframe to assist administrators through the PII removal process.

PBGC Connect does not protect against unauthorized access to PII. The vulnerability of PII in PBGC Connect exposes PBGC to increased risk of the Privacy Act of 1974, 5 U.S.C. 552a being violated – i.e., PII disclosures, and not reported as they are unaware of the violation.

Recommendations:

- With OIT's technical assistance, all business units should implement the default site policies and guidelines provided by the PBGC Connect Governance Council. Additionally, business areas should implement any additional, business-specific guidance required for their sites. **(OIG Control Number FISMA-14-01)**

- All business units using PBGC Connect should implement policies and guidelines to restrict users from storing structured, application-derived data inappropriately in PBGC Connect. **(OIG Control Number FISMA-14-02)**

- PBGC should implement a tool that has preventive control capability to block documents containing PII from being uploaded to sites that are not CUI-tagged. **(OIG Control Number FISMA-14-03)**

- PBGC should refine and finalize *SharePoint Fast Search & PII Data Daily Check* to include the timeframe for the removal of PII, and management oversight to confirm timely removal of PII. **(OIG Control Number FISMA-14-04)**

- Determine whether the existence of PII in PBGC Connect that are not in the proper Controlled Unclassified Information sites is a violation of the Privacy Act. If so, assess the violation and make the appropriate reports of Privacy Act disclosures. **(OIG Control Number FISMA-14-05)**

2. Plan of Action and Milestones (POA&M)

PBGC's POA&M process is not mature and effective. This is a longstanding issue; PBGC is still working on the process of consolidating its POA&Ms into an agency-wide POA&M. The processes are not fully developed and implemented, therefore, this finding continues for FY 2014.

PBGC implemented the Cyber Security Assessment and Management (CSAM) in 2013 as part of its effort to improve the tracking and maintaining of security weaknesses. CSAM has tracking, reporting and notification capabilities that can improve the POA&M management process. The CSAM POA&M management process outlines weaknesses and delineates the tasks necessary to mitigate them, including: planning and monitoring corrective actions; defining roles and responsibilities for weakness resolution; assisting in identifying the security funding requirements necessary to mitigate weaknesses; tracking and prioritizing resources; and informing decision makers. Currently, Financial Operations Department (FOD) does not fully utilize CSAM to track and maintain POA&Ms for its systems: Consolidated Financial Systems (CFS), Trust Accounting System (TAS), and My Plan Administration Account (MyPAA). TAS's Information Security Officer has not attended CSAM training. CSAM is currently in pilot and will be officially deployed in FY 2015.

FOD is the only department that tracks and maintains its POA&Ms in Excel spreadsheets, which are reported to the Enterprise Cybersecurity Division (ECD), through a quarterly POA&M data call. ECD then uses those Excel spreadsheets to update CSAM with new POA&Ms and status.

Recommendations:

- Develop, maintain and update PBGC's entity-wide plan of action and milestones, at least on a quarterly basis, and ensure it includes all entity-wide security deficiencies noted. **(OIG Control Number FISMA-09-08)**

  PBGC's Scheduled Completion Date: 06/15/2014

- Disseminate PBGC's entity-wide POA&M to all responsible parties to ensure corrective actions are taken in accordance with POA&M. **(OIG Control Number FISMA-09-09)**

  PBGC's Scheduled Completion Date: 06/15/2014

- Establish controls to ensure that FOD's POA&Ms are tracked appropriately and updated regularly in CSAM in accordance with FODs Continuous Monitoring program. **(OIG Control Number FISMA-14-06)**

- OIT should finalize the deployment of CSAM as the official system of record for POA&M management. **(OIG Control Number FISMA-14-07)**

- Ensure all personnel involved in the POA&M management process receive the proper CSAM training. **(OIG Control Number FISMA-14-08)**

3. Shared Accounts

Four General Accounting Branch (GAB) staff (two accountants, one team lead, and one Branch Chief) with different levels of approval authority share one Comprizon User ID and password to approve requisitions. PBGC has not enforced controls to restrict and eliminate shared IDs and passwords in the Comprizon application.

Recommendations:

- Assign separate accounts to each individual who needs access to Comprizon. **(OIG Control Number FISMA-14-09)**

4. Information Security Continuous Monitoring (ISCM) Program

PBGC has not established and implemented an entity-wide continuous monitoring strategy and program to assist PBGC in the active and consistent maintenance of ongoing awareness of its information security, vulnerabilities, and threats to support organizational risk management decisions. PBGC continues to procure, implement, and deploy technical tools to support the full implementation of the ISCM program. However, PBGC has not documented its ISCM strategy. In the interim, the Financial Operations Department within PBGC has established a continuous monitoring plan and program for certain financial management systems (Consolidated Financial Systems, Trust Accounting System, and My Plan Administration Account).

PBGC's Chief Information Security Officer (CISO) recently established a 150-day plan to re-establish goals and objectives to improve PBGC's cybersecurity efforts with an estimated entity-wide ISCM program implementation by second quarter of fiscal year 2015.

Recommendations:

- Establish and document an entity-wide ISCM strategy using PBGC risk assessments. **(OIG Control Number FISMA-14-10)**

- Establish and implement a consistent entity-wide ISCM program in accordance with PBGC's ISCM strategy, to include metrics assisting PBGC in evaluating and controlling ongoing risks. **(OIG Control Number FISMA-14-11)**

5. PBGC Security Clearance – High Risk Designation

Critical security personnel do not have top secret clearances to enable them to attend briefings by DHS and National Security Agency (NSA) on emerging security threats.

The lack of individuals with Top Secret clearance restricts security officials from being informed about incidents such as the breach of the U.S. Postal Service that took place in September 2014 and disclosed in November 2014. PBGC security officials were not aware of the breach until it was published by the Washington Post.

In addition, PBGC security officials were not able to attend a threat briefing by the Information Security and Identity Management Committee on December 17, 2014, because they did not have the required security clearance to attend.

Recommendations:

- PBGC should review IT security personnel positions and assess which require a top secret clearance to effectively perform the job. **(OIG Control Number FISMA-14-12**)

- Upon identifying the positions that require access to Top Secret information, ensure the position descriptions appropriately describe the need and reassess the position designation. **(OIG Control Number FISMA-14-13)**

- Seek top secret clearance for PBGC personnel that require such clearance for their position designation. **(OIG Control Number FISMA-14-14)**

6. PBGC Reinvestigation

PBGC does not conduct background reinvestigations when employees have changed jobs or roles to one in which the position risk designation is assessed at a higher level. Positions at the High and Moderate risk levels are referred to as "Public Trust" positions. Public Trust positions involve access to, operation or control of proprietary systems of information, such as financial or personal records, with a significant risk for causing damage to people, programs or an agency, or for realizing personal gain. There are three suitability position risk levels, defined and explained in the table below:

LEVELS	DEFINITIONS AND REPRESENTATIVE DUTIES OR RESPONSIBILITIES
HIGH **(HR)** **Public Trust Position**	**Positions with the potential for *exceptionally serious impact* on the integrity and efficiency of the service.** Duties involved are especially critical to the agency or program mission with a broad scope of responsibility and authority. Positions include: • Policy-making, policy-determining, and policy-implementing; • Higher level management duties or assignments, or major program responsibility; • Independent spokespersons or non-management position with authority for independent action; • Investigative, law enforcement, and any position that requires carrying a firearm; and • Fiduciary, public contact, or other duties demanding the highest degree of public trust
MODERATE **(MR)** **Public Trust Position**	**Positions with the potential for *moderate to serious impact* on the integrity and efficiency of the service.** Duties involved are considerably important to the agency or program mission with significant program responsibility or delivery of service. Positions include: • Assistants to policy development and implementation; • Mid-level management duties or assignments; • Any position with responsibility for independent or semi-independent action; and • Delivery of service positions that demand public confidence or trust.
LOW **(LR)**	**Positions that involve duties and responsibilities of *limited relation* to an agency or program mission, with the potential for *limited impact* on the integrity and efficiency of the service.**

Per our review, three out of five employees sampled who have changed jobs or roles did not have the appropriate level of background investigation to perform their new job functions. Background reinvestigations were not initiated for these employees before or after the effective date of their position change to ensure that employees in a new job/role that had been assessed at a higher risk designation had the appropriate level of reinvestigation performed.

Recommendations:

- Develop, document and implement a process for the timely assessment of employees and contractors transferred or promoted to a new position or role to determine whether the risk-level has changed. **(OIG Control Number FISMA-14-15)**

- Conduct assessment of current PBGC employees and contractors to determine whether they have been transferred or promoted to a new position or role since their last background investigation. **(OIG Control Number FISMA-14-16)**

- For those PBGC employees and contractors who have new roles or responsibilities, conduct the risk-level assessment to determine whether a different level of background investigation is required. **(OIG Control Number FISMA-14-17)**

- For PBGC employees and contractors for whom it is determined that new roles or responsibilities are at a higher risk level, conduct the appropriate background investigation. **(OIG Control Number FISMA-14-18)**

7. PBGC IP Address Inventory

PBGC did not use a centralized tracking repository to identify and manage its inventory of Internet protocol (IP) addresses connected to the network, and identify assets for version control. Therefore, PBGC did not maintain an accurate inventory. Furthermore, vulnerability scans were incomplete. Patches and configuration changes based upon scan results were also incomplete. PBGC could not determine what assets were missing from its scans or what types of vulnerabilities were within its environment.

PBGC reported a total count of 4,932 connected hardware assets for the PBGC unclassified network in the Chief Information Officer 2014 FISMA Report. PBGC used two separate systems to account for hardware assets. PBGC then compiled the two lists into one to account for all assets connected to the PBGC network.

After conducting separate scans of the PBGC network, both PBGC's Patch and Vulnerability Management Group (PVMG) and CLA reported differing counts of IP addresses. Neither the PVMG nor CLA counts reconciled with PBGC's hardware asset listing.

Recommendations:

- Assess PBGC's current process and critical control points in identifying all assets connected to the PBGC network. Determine the shortcomings in PBGC's current process to compile an accurate and comprehensive inventory of all assets and connections to the PBGC network. **(OIG Control Number FISMA-14-19)**

- Reconcile PBGC's IP address inventory with the independent IP address inventory determined by the annual OIG assessment. Determine why differences exist and develop and implement a strategy to reconcile and eliminate differences in the IP address inventory count. **(OIG Control Number FISMA-14-20)**

- Develop and implement a plan of action to identify an accurate and comprehensive inventory of PBGC's IP addresses and all connections to the PBGC network. **(OIG Control Number FISMA-14-21)**

8. Application Specific General Controls

In FY 2013, we noted the following weaknesses in the general controls designed to protect the Pension Insurance Modeling System (PIMS) application.

- A risk assessment has not been conducted for PIMS.
- PIMS does not have an established Contingency Plan in place to recover the PIMS application and database following a disruption. PBGC cannot perform modeling and make projections, if PIMS is not available.
- PIMS does not have a Continuity of Operations Plan (COOP) as PBGC has not considered PIMS a mission critical application.
    - Policy, Research and Analysis Department (PRAD) had recorded in the FY 2012 Business Impact Analysis that PIMS produces the forecasts of potential financial positions of insurance programs. However, PIMS is not listed as a required IT component.
- PIMS is not adequately supported by PBGC's general support systems and does not fully inherit common controls from these systems.

- PRAD has not adopted and implemented PBGC's *Life Cycle Security Standard* in its maintenance of PIMS.
- Technical controls have not been implemented to separate incompatible duties in PIMS.
- A SA&A is planned for PIMS, but had not started as of 9/30/14.

Recommendations:

- Complete a security risk assessment for PIMS. **(OIG Control Number FISMA-13-08)**

- Ensure that PIMS is included in the PBGC COOP. **(OIG Control Number FISMA-13-10)**

- Develop and document a Contingency Plan for PIMS. **(OIG Control Number FISMA-13-11)**

- Ensure that PIMS is adequately supported by PBGC's general support systems and inherits common controls from these systems. **(OIG Control Number FISMA-13-12)**

- PRAD should adopt and implement PBGC's Life Cycle Security Standard in its maintenance of PIMS. **(OIG Control Number FISMA-13-14)**

- Develop and implement technical controls to separate incompatible duties in PIMS**. (OIG Control Number FISMA-13-15)**

- Conduct a Security Assessment and Authorization (SA&A) review process for PIMS. **(OIG Control Number FISMA-13-16**)

9. Review of Interconnection Security Agreements

In FY 2013, PBGC's process for documenting its interconnection security agreements with other entities had outdated documents and incomplete attachments; the tracking document was also incomplete. No progress was made to address this finding in FY 2014. The specific weaknesses noted were as follows:

- Three instances where the interconnecting agency's Authorization to Operate had expired;
    - Department of Commerce (DoC) National Technical Information Service (NTIS) eALG
    - Internal Revenue Service (IRS) Health Coverage Tax Credit (HCTC) Program
    - Department of Interior (DoI) Interior Business Center (IBC) Federal Payroll and Personnel System (FPPS)
- One instance where the ISA Checklist did not accurately reflect the expiration date;
    - Social Security Administration (SSA) DeathMatch; and
- One instance where the ISA was incomplete (appendices were not included).
    - Social Security Administration (SSA) DeathMatch.

Recommendations:

- Ensure the Information Security Agreement Tracking Document is reviewed for accuracy and completeness. **(OIG Control Number FISMA-13-17)**

- Review the Information Security Agreements to ensure they are current and complete. **(OIG Control Number FISMA-13-18)**

VII. FISMA-RELATED FINDINGS REPORTED IN THE FINANCIAL STATEMENT AUDIT

The following table summarizes FISMA-related findings noted under entity-wide security program planning and management, access controls, and configuration management, that were reported in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2014 and 2013 Financial Statements Audit* (AUD-201-3 /FA-14-101-3) issued November 14, 2014.

Finding Summary	Recommendation
1. 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.	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)***
2. Common security controls provide the foundation for the effectiveness of enterprise-wide system security operations. In FY 2014, PBGC continued to change its	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 #**

Finding Summary	Recommendation
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.	**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)***
3. 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	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

Finding Summary	Recommendation
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.	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) ***
4. 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	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)***

Finding Summary	Recommendation
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.	
5. 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.	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-**

Finding Summary	Recommendation
	11) (PBGC scheduled completion date: July 31, 2014)
6. 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.	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)****
7. 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'	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)****

	Finding Summary	Recommendation
	Risk Acceptance Forms did not directly address account dormancy. Once notified, PBGC revised these Risk Acceptance Forms to address account dormancy.	
8.	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.	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)***
9.	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	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

Finding Summary	Recommendation
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: o Incident handling process was ineffective in monitoring, detecting, examining and reporting security incidents. o Security incident policies and procedures were not reviewed annually in accordance with PBGC's policies. o Incident handling process was not reviewed to ensure effectiveness of	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)**

Finding Summary	Recommendation
PBGC's security event categorization procedures and decision process, review of IDS logs, and other continuous monitoring activity. o 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. o 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). o 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. o 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. o Directive IM 10-3, Protecting Sensitive Information, was not updated to provide updated guidance on protecting sensitive information.	

* PBGC has not established a revised completion date.

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

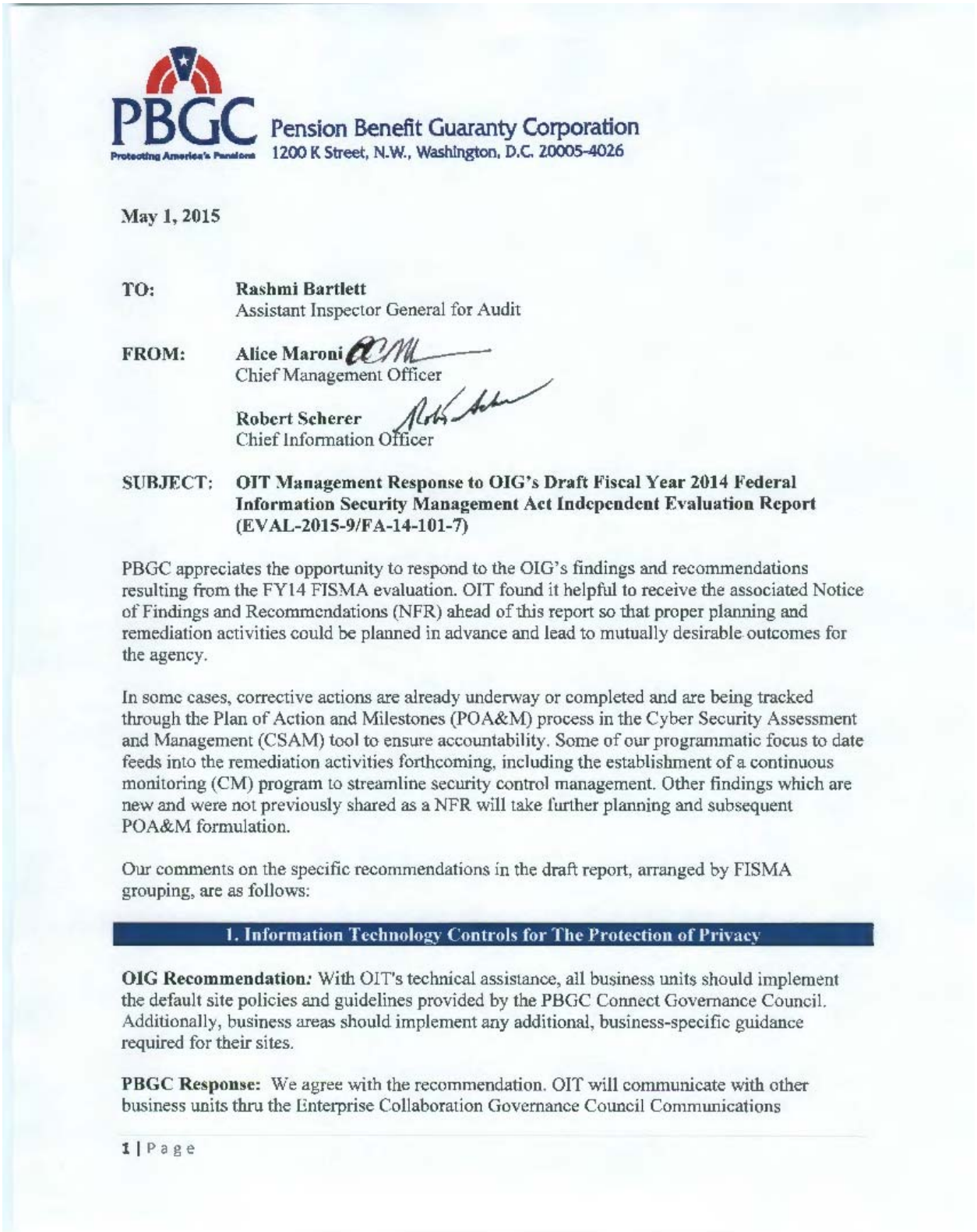
VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2014

OIG Control Number	Date Closed	Original Report Number
FISMA-09-10		AUD-2010-6/FA-09-64-6
FISMA-09-11		AUD-2010-6/FA-09-64-6
FISMA-11-05		EVAL-2012-9/FA-11-82-7
FISMA-13-09		EVAL-2014-9/FA-13-93-7
FISMA-13-13		EVAL-2014-9/FA-13-93-7

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

OIG Control Number	Original Report Number
Prior Year	
FISMA-09-08	AUD-2010-6/FA-09-64-6
FISMA-09-09	AUD-2010-6/FA-09-64-6
FISMA-11-02	EVAL-2012-9/FA-11-82-7
FISMA-13-08	EVAL-2014-9/FA-13-93-7
FISMA-13-10	EVAL-2014-9/FA-13-93-7
FISMA-13-11	EVAL-2014-9/FA-13-93-7
FISMA-13-12	EVAL-2014-9/FA-13-93-7
FISMA-13-14	EVAL-2014-9/FA-13-93-7
FISMA-13-15	EVAL-2014-9/FA-13-93-7
FISMA-13-16	EVAL-2014-9/FA-13-93-7
FISMA-13-17	EVAL-2014-9/FA-13-93-7
FISMA-13-18	EVAL-2014-9/FA-13-93-7
Current Year	
FISMA-14-01	EVAL 2015-9/FA-14-101-7
FISMA-14-02	EVAL 2015-9/FA-14-101-7
FISMA-14-03	EVAL 2015-9/FA-14-101-7
FISMA-14-04	EVAL 2015-9/FA-14-101-7
FISMA-14-05	EVAL 2015-9/FA-14-101-7
FISMA-14-06	EVAL 2015-9/FA-14-101-7
FISMA-14-07	EVAL 2015-9/FA-14-101-7
FISMA-14-08	EVAL 2015-9/FA-14-101-7
FISMA-14-09	EVAL 2015-9/FA-14-101-7
FISMA-14-10	EVAL 2015-9/FA-14-101-7
FISMA-14-11	EVAL 2015-9/FA-14-101-7
FISMA-14-12	EVAL 2015-9/FA-14-101-7
FISMA-14-13	EVAL 2015-9/FA-14-101-7
FISMA-14-14	EVAL 2015-9/FA-14-101-7
FISMA-14-15	EVAL 2015-9/FA-14-101-7
FISMA-14-16	EVAL 2015-9/FA-14-101-7
FISMA-14-17	EVAL 2015-9/FA-14-101-7
FISMA-14-18	EVAL 2015-9/FA-14-101-7
FISMA-14-19	EVAL 2015-9/FA-14-101-7
FISMA-14-20	EVAL 2015-9/FA-14-101-7
FISMA-14-21	EVAL 2015-9/FA-14-101-7

X. MANAGEMENT RESPONSE



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

May 1, 2015

TO: **Rashmi Bartlett**
Assistant Inspector General for Audit

FROM: **Alice Maroni**
Chief Management Officer

Robert Scherer
Chief Information Officer

SUBJECT: **OIT Management Response to OIG's Draft Fiscal Year 2014 Federal Information Security Management Act Independent Evaluation Report (EVAL-2015-9/FA-14-101-7)**

PBGC appreciates the opportunity to respond to the OIG's findings and recommendations resulting from the FY14 FISMA evaluation. OIT found it helpful to receive the associated Notice of Findings and Recommendations (NFR) ahead of this report so that proper planning and remediation activities could be planned in advance and lead to mutually desirable outcomes for the agency.

In some cases, corrective actions are already underway or completed and are being tracked through the Plan of Action and Milestones (POA&M) process in the Cyber Security Assessment and Management (CSAM) tool to ensure accountability. Some of our programmatic focus to date feeds into the remediation activities forthcoming, including the establishment of a continuous monitoring (CM) program to streamline security control management. Other findings which are new and were not previously shared as a NFR will take further planning and subsequent POA&M formulation.

Our comments on the specific recommendations in the draft report, arranged by FISMA grouping, are as follows:

1. Information Technology Controls for The Protection of Privacy

OIG Recommendation: With OIT's technical assistance, all business units should implement the default site policies and guidelines provided by the PBGC Connect Governance Council. Additionally, business areas should implement any additional, business-specific guidance required for their sites.

PBGC Response: We agree with the recommendation. OIT will communicate with other business units thru the Enterprise Collaboration Governance Council Communications

1 | Page

subcommittee to ensure that they are aware of the requirement to adhere to default site policies and guidelines or establish their own site-specific policies and guidelines in accordance with PBGC Connect Governance. OIT will provide technical assistance with the implementation of all default policies and guidelines and will provide additional technical assistance for site-specific policies and guidelines upon request. OIT will incorporate PBGC Connect training into its Security Awareness Training program. Expected timeline for implementation is March 2016.

OIG Recommendation: All business units using PBGC Connect should implement policies and guidelines to restrict users from storing structured, application-derived data inappropriately in PBGC Connect.

PBGC Response: We agree with the recommendation. OIT will work with the Enterprise Collaboration Governance Council to establish the appropriate default site policy and guidelines to include governance that instructs users not to store structured, application-derived data inappropriately in PBGC Connect. OIT will communicate with other business units thru the Enterprise Collaboration Governance Council Communications subcommittee to ensure that they are aware of the updated governance instructing users to not store structured, application-derived data inappropriately in PBGC Connect. Expected timeline for implementation is March 2016.

OIG Recommendation: PBGC should implement a tool that has preventive control capability to block documents containing PII from being uploaded to sites that are not CUI-tagged.

PBGC Response: We agree with the recommendation. PBGC agrees that a tool is necessary to quickly identify and remediate inappropriate placement of documents containing PII. PBGC is currently testing a tool that fulfills this requirement. The tool can be configured so that as PII exposures on SharePoint are identified, the documents are automatically routed to a secure repository to prevent unauthorized access. Expected timeframe for full implementation of the tool is during second quarter FY2016. It should be noted that, while we believe the tool we are implementing is a good solution and addresses the need outlined in the recommendation, it is a not a tool that proactively blocks documents containing PII. Based on our research, the category of data loss prevention tools that would block the inappropriate uploading of PII requires significant investment, is not currently funded nor included in acquisition planning and - due to their client-side nature - may have implications for expeditious business processing. After full implementation of the "identify and remediate" tool, PBGC looks forward to further discussions as to whether the underlying condition has been addressed or if a truly preventative tool is required.

OIG Recommendation: PBGC should refine and finalize SharePoint FastSearch & PII Data Daily Check to include the timeframe for the removal of PII, and management oversight to confirm timely removal of PII.

PBGC Response: We agree with the recommendation. OIT will update the work instruction to direct OIT personnel to properly secure any PII data identified within 48 hours of initial detection should the business area decline to take action when notified of a compliance issue. OIT will also train the relevant personnel on the changes to the work instruction. OIT Federal Management will periodically review the PII detection and removal process to ensure

compliance with the required timeframe. Expected timeframe for completion is June 30, 2015.

OIG Recommendation: Determine whether the existence of PII in PBGC Connect that are not in the proper Controlled Unclassified Information sites is a violation of the Privacy Act. If so, assess the violation and make the appropriate reports of Privacy Act Disclosures.

PBGC Response: We agree with the recommendation. However, PBGC notes that this recommendation is new to this report. OIT determined that instances of PII in PBGC Connect that are not in the proper Controlled Unclassified Information (CUI) sites are violations of the Privacy Act. OIT assessed and reported the previously identified violation to the PBGC Privacy Office and will do so in the future, should additional instances arise. Further, OIT will update its work instruction, SharePoint Fast Search & PII Data Daily Check, to include a requirement to report all instances of improperly stored PII in PBGC Connect to the PBGC Privacy Office. The scheduled completion date for these activities is June 30, 2016.

2. Plan of Action and Milestones (POA&M)

OIG Recommendation: Establish controls to ensure that FOD's POA&Ms are tracked appropriately and updated regularly in CSAM in accordance with FODs Continuous Monitoring program.

PBGC Response: We agree with the recommendation. PBGC deployed CSAM as the system of record for POA&Ms on January 5, 2015 and has been improving the POA&M process to best utilize the functionality of CSAM. All business areas, including FOD, have been utilizing CSAM for POA&M tracking.

OIG Recommendation: OIT should finalize the deployment of CSAM as the official system of record for POA&M management.

PBGC Response: We agree with the recommendation. PBGC deployed CSAM as the system of record for POA&Ms on January 5, 2015. ECD continues to improve the POA&M process to best utilize available CSAM functionalities, and ensures POA&Ms are accounted for within CSAM. OIT plans to submit an RCF for POA&M related weaknesses for consideration in the FY15 OIG audit. The scheduled completion date is June 30, 2015.

OIG Recommendation: Ensure all personnel involved in the POA&M management process receive proper CSAM training.

PBGC Response: We agree with the recommendation. Representatives and from all business areas have been trained on the tool and POA&Ms are accounted for within CSAM. Management expects to submit an RCF for POA&M related weaknesses for consideration in the FY15 OIG audit. Scheduled completion date is June 30, 2015.

3. Shared Accounts

OIG Recommendation: Assign separate accounts to each individual who needs access to Comprizon.

PBGC Response: We agree with the recommendation. FOD Management agrees with the recommended corrective action. The GAB accountant logs into Comprizon using a unique user id and password assigned by Procurement Department system personnel. This implemented procedures continues even in the absence of key personnel as unique user ids and workflow routing are maintained by a forward feature within the Comprizon system. The GAB Supervisor also logins to Comprizon using a unique assigned user id and password. The scheduled completion date for these activities is June 30, 2015.

4. Information Security Continuous Monitoring (ISCM) Program

OIG Recommendation: Establish and document an entity-wide ISCM strategy using PBGC risk assessments.

PBGC Response: We agree with the recommendation. A POA&M #574 in Cyber Security Assessment and Management (CSAM) has been established to track the Information Security Continuous Monitoring (ISCM) program implementation progress. Ongoing progress will document and produce an enterprise ISCM strategy, policy, communications plan, controls assessment and schedule plan and metrics with stakeholder reporting. The scheduled completion date for these activities is June 30, 2015.

OIG Recommendation: Establish and implement a consistent entity-wide ISCM program in accordance with PBGC's ISCM strategy, to include metrics assisting PBGC in evaluating and controlling ongoing risks.

PBGC Response: We agree with the recommendation. A POA&M #574 in Cyber Security Assessment and Management (CSAM) has been established to track the Information Security Continuous Monitoring (ISCM) program implementation progress. Collaborating with PBGC business areas, OIT will complete establishing an enterprise wide ISCM program, which includes concept of operation, policy, communications plan, controls assessment, metrics, etc. The scheduled completion date for completing this recommendation is June 30, 2015.

5. PBGC Security Clearance – High Risk Designation

OIG Recommendation: PBGC should review IT security personnel positions and assess which require a top secret clearance to effectively perform the job.

PBGC Response: We agree with the recommendation. PBGC is dedicated to meeting the challenges facing our information security workforce and a number of improvements will be made. The first step is to ensure PBGC has the ability to access and share cyber threat information, at a minimum, at the corporation level. This involves identifying positions that need security clearance within the appropriate ECD, OIG, WSD. OIT and WSD will jointly conduct an assessment to identify individuals needing clearance so that individuals can perform their jobs effectively. PBGC plans on completing this identification by December 31, 2015.

OIG Recommendation: Upon identifying the positions that require access to Top Secret information, ensure the position descriptions appropriately describe the need and reassess the position designation.

PBGC Response: We agree with the recommendation. Upon completion of identifying those needing security clearance, OIT and WSD will ensure those position designations be updated appropriately. PBGC plans on completing those updates by June 30, 2016.

OIG Recommendation: Seek top secret clearance for PBGC personnel that require such clearance for their position designation.

PBGC Response: We agree with the recommendation. PBGC will begin the process of seeking viable sponsorship through ODNI. We plan to identify a sponsor and establish a clearance process. Pending sponsorship, our plan to accomplish this task is through an inter-agency agreement. Upon completion, PBGC will be able to process and maintain the appropriate security clearance for individuals needing this designation to perform their jobs effectively. PBGC plans on completing such an agreement by November 30, 2016.

6. PBGC Reinvestigation

OIG Recommendation: Develop, document and implement a process for the timely assessment of employees and contractors transferred or promoted to a new position or role to determine whether the risk-level has changed.

OIG Recommendation: Conduct assessment of current PBGC employees and contractors to determine whether they have been transferred or promoted to a new position or role since their last background investigation.

OIG Recommendation: For those PBGC employees and contractors who have new roles or responsibilities, conduct the risk-level assessment to determine whether a different level of background investigation is required.

OIG Recommendation: For PBGC employees and contractors for whom it is determined that new roles or responsibilities are at a higher risk level, conduct the appropriate background investigation.

PBGC Response: We agree with the above four (4) recommendations. The following is a current description of activities completed in response to these findings and supersedes the management response originally submitted in December 2014.

Federal Employee Transfers

WSD is notified by HRD bi-weekly documenting all Federal transfers and promotions. WSD takes the new position and risk level data and conducts a reconciliation with PBGC's personnel security database and OPM's Central Verification System to determine if the Federal employee's current background investigation is at the risk level assigned to the new position. If the Federal

employee's current background investigation is not at the risk level of the new position, then WSD will initiate a new background investigation for that employee. To ensure the reporting process stays on track, WSD established a recurring calendar reminder for WSD personnel involved in the reporting process and also keeps a detailed tracking spreadsheet.

Contractor Transfers

WSD is notified by the COR when a contractor transfers from one contract to another. This process is initiated on the Separation Clearance for Contractor Employees (169C). Once the 169C is received, the Security Team reaches out to the COR to confirm risk level changes on the new contract. If risk level changes are not required, no further action is taken. If risk level changes are required, the contractor is contacted and a new background investigation is initiated. It is the responsibility of the COR to provide WSD with notification of a contractors new roles or responsibilities that will require a higher level background investigation. The contractor transfers are documented on a detailed spreadsheet and WSD maintains the 169C.

In accordance with the above, the WSD Security Processing Manual was updated effective April 23, 2015. The scheduled completion date for submitting RCFs for these activities is June 30, 2015.

7. PBGC IP Address Inventory

OIG Recommendation: Assess PBGC's current process and critical control points in identifying all assets connected to the PBGC network. Determine the shortcomings in PBGC's current process to compile an accurate and comprehensive inventory of all assets and connections to the PBGC network.

PBGC Response: We agree with the recommendation. OIT will conduct a thorough assessment of the current process utilized to compile a comprehensive and accurate inventory of all assets and connections to the PBGC network. There is a current GSS POA&M which addresses this issue (POA&M #1237 CM-8: GSS System Component Tracking). PBGC will engage with the IG as significant milestones, such as the completion of the assessment, are completed. The scheduled completion date for these activities is June 30, 2016.

OIG Recommendation: Reconcile PBGC's IP address inventory with the independent IP address inventory determined by the annual OIG assessment. Determine why differences exist and develop and implement a strategy to reconcile and eliminate differences in the IP address inventory count.

PBGC Response: We agree with the recommendation. As PBGC improves its IP address inventory process and results, it will compare its IP address inventory with the inventory from the annual OIG assessment and determine the cause(s) for any discrepancies. There is a GSS POA&M which addresses this issue (POA&M #1237 CM-8: GSS System Component Tracking). After the completion of the assessment, PBGC will be able to determine a more definitive date by which reconciliation will take place. The scheduled completion date for these activities is June 30, 2016.

OIG Recommendation: Develop and implement a plan of action to identify an accurate and comprehensive inventory of PBGC's IP addresses and all connections to the PBGC network.

PBGC Response: We agree with the recommendation. OIT will develop and implement a plan to remediate deficiencies in the current process utilized to provide a complete and accurate inventory of IP networks, connected hosts, and interconnections. There is a GSS POA&M which addresses this issue (POA&M #1237 CM-8: GSS System Component Tracking). After the completion of the assessment, PBGC will be able to determine a more definitive date by the inventory process will be improved sufficiently to request closure of these findings. The scheduled completion date for these activities is June 30, 2016.

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