Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation Report

Fiscal Year 2016 Federal Information Security Modernization Act Independent Evaluation Report

March 22, 2017

EVAL 2017-9/FA-16-110-7

Office of Inspector General
Pension Benefit Guaranty Corporation

March 22, 2017

TO: Thomas Reeder
Director

FROM: Nina Murphy
Assistant Inspector General for Audits

SUBJECT: Fiscal Year 2016 Federal Information Security Modernization Act Independent Evaluation Report (EVAL 2017-9/FA-16-110-7)

I am pleased to transmit the fiscal year 2016 Federal Information Security Modernization Act (FISMA) Independent Evaluation report detailing the results of our review of the 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 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 largely agreed with the 20 new recommendations in this report. We will work with the Corporation in the coming weeks to resolve each recommendation and reach an agreed-to management decision for corrective action.

We would like to take this opportunity to express our appreciation for the overall cooperation CliftonLarsonAllen and OIG received during the audit.

Attachment

cc: Marty Boehm
Cathleen Kronopolus
Karen Morris
Judith Starr
Patricia Kelly
Alice Maroni
Robert Scherer

CliftonLarsonAllen

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

Robert A. Westbrooks
Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, NW
Washington, DC 20005-4026

Dear Mr. Westbrooks:

We are pleased to provide the Fiscal Year (FY) 2016 Federal Information Security Modernization 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 to conduct annual evaluations of their agency's security programs and practices, and to report the results of their evaluations to the Office of Management and Budget (OMB). OMB Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements* 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 PBGC's OIG. The OIG then reviewed, approved, and submitted the responses to OMB on November 10, 2016. This evaluation report provides additional information on the results of our review of the PBGC information security program and information systems.

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 February 28, 2017) to the draft FISMA 2016 Independent Evaluation Report.

The projection of any conclusions, based on our findings, to future periods is subject to the risk that the conclusion may no longer be accurate because of changes in conditions or compliance with controls.

CliftonLarsonAllen LLP

Calverton, Maryland
February 28, 2017

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization Act (FISMA) requires agencies to adopt a risk-based, life-cycle approach to improve computer security, which 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.

We are reporting 24 FISMA findings with 30 recommendations of which 20 are new for FY 2016 based on the results of our FY 2016 independent evaluation. In addition to those in this report, there were eight FISMA-related recommendations reported in the Corporation's FY 2016 internal control report based on our FY 2016 financial statements audit work. There is no overlap in the findings and recommendations in the two reports. Pension Benefit Guaranty Corporation (PBGC) took corrective actions on information technology (IT) recommendations from our financial statement internal control reports and prior FISMA reports; however, based on the issues identified and the continued existence of unremediated recommendations, we concluded that PBGC's information security program still needs improvement.

II. BACKGROUND

The PBGC protects the pensions of more than 41 million workers and retirees in more than 24,000 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 are major priorities for PBGC. Although 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, 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 the Department of Homeland Security (DHS) to administer FISMA; OMB retains policy/procedure authority. DHS can issue "binding operational directives" (compulsory for agencies) and coordinates with the National Institute of Standards and Technology (NIST) to avoid conflicts. The Act also increases focus on detecting, reporting, and responding to security incidents; for example, Congress must be notified of a “confirmed” breach within seven days. OMB revised Circular No. A-130, *Managing Information as a Strategic Resource*, effective July 28, 2016, to reflect changes in law and advances in technology. It was revised to represent a shift in security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.

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.

PBGC OIG contracted with CliftonLarsonAllen LLP (CLA) to conduct PBGC's FY 2016 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 (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.
- Government Accountability Office’s (GAO) *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)
- Premium & Practitioner System (PPS)
- Pension Insurance Modeling System (PIMS)
- Pension 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 8, 2016 to September 30, 2016, at PBGC's headquarters in Washington, DC.

This independent evaluation was prepared based on information available as of September 30, 2016.

V. SUMMARY OF CURRENT YEAR TESTING

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 made significant progress in addressing the security weaknesses noted in prior years; however, much work remains to continue correcting these deficiencies. In this year's audit, we identified 10 new weaknesses; some recommendations remain from prior years and are noted below:

1. Entity-Wide Security Program Planning and Management

PBGC continued to make progress in addressing the Corporation's entity-wide security program planning and management control deficiencies, but these efforts have not resulted in a fully implemented and effective entity-wide information security program as required under OMB and NIST guidance. These requirements provide a framework for assessing and managing risks, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of the Corporation's sensitive or critical resources.

In FY 2016, PBGC developed and published the PBGC Risk Management Framework (RMF) process to transition and fully implement an entity-wide information security risk management program. The RMF will address both security and privacy controls when fully implemented. PBGC's IT risk management process focused on identifying and evaluating the threats and vulnerabilities. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. PBGC was proactive in addressing new federal guidance on IT security and privacy and in developing corrective actions to address potential control gaps. In addition, PBGC developed and started implementing a plan to be fully compliant with OMB Circular A-130.

2. Access Controls and Configuration Management

PBGC also made progress in addressing access controls and configuration management deficiencies identified in previous years, but some security weaknesses remain. Weaknesses in the PBGC IT environment continue to contribute to deficiencies in system configuration, segregation of duties, and role-based access controls based on least privilege.

In FY 2016, PBGC continued to implement various tools and processes to establish a more coherent environment for access controls and configuration management security controls. PBGC, however, revised the completion dates for many planned corrective actions by one year or more. We will continue to make the recommendations to address the underlying access controls and configuration management weaknesses in PBGC's information system security controls.

Our evaluation also found deficiencies specifically related to responses required in OMB M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*, dated November 4, 2016, which are included in this report. These findings and recommendations, not previously reported, are as follows:

- Continuous Monitoring Management
- Configuration Management
- Identity and Access Management
- Incident Response and Reporting
- Risk Management
- Security Training
- Contingency Planning

VI. FINDINGS AND RECOMMENDATIONS

1. Continuous Monitoring Management

a. Security Information and Event Management

PBGC's *Security Incident Management (SIM) Plan*, dated May 2016, indicates that the analysts will complete a review of all security events in queue starting with the most critical events and decreasing in severity. This event analysis will be completed on a monthly basis and reviewed by the SIM Program Manager.

PBGC had not fully implemented its security information and event management (SIEM) capability to include PBGC's major applications. The current implementation only extended to the general support systems. System owners of major applications had not determined the requirements for data collection, storage, indexing, searching, correlating, visualizing, analyzing and reporting. Consequently, PBGC's implementation of its SIEM tool has not matured to fully maximize its capabilities. PBGC does not have adequate coverage of its information technology environment to adequately monitor its security status and events.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* states:

> The implementation and effective use of SIEM technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53 security controls including AC-5, Separation of Duties; AU-2, Auditable Events; AU-6, Audit Review, Analysis, and Reporting; AU-7, Audit Reduction and Report Generation; CA-2, Security Assessments; CA-7, Continuous Monitoring; IR-5, Incident Monitoring; PE-6, Monitoring Physical Access; RA-3, Risk Assessment; RA-5, Vulnerability Scanning; and SI-4, Information System Monitoring.

In FY 2016, PBGC developed the security requirements necessary to resolve security information and event management weaknesses and now is in the process of developing additional controls to complete remediation activities.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Fully implement Splunk Enterprise in PBGC, including its SIEM capability. **(OIG Control Number FISMA-15-01)**

- Require system owners to fully implement Splunk Enterprise for PBGC major applications. **(OIG Control Number FISMA-15-02)**

- Ensure the consistent use of the Event Analysis Checklist as part of the event analysis process. **(OIG Control Number FISMA-15-03)**

2. Configuration Management

a. Windows File Transfer Protocol (FTP)

Window servers were operating with FTP, despite PBGC's plans to validate that FTP had been removed from all servers by October 1, 2015. The use of FTP is insecure as data is transmitted as plaintext, which presents a risk of PBGC disclosing information to unauthorized persons. Our FY 2016 scan results show that PBGC had not removed FTP from all servers in the production environment. As a result, these servers did not meet PBGC's configuration baselines and are at risk for unauthorized disclosure.

Recommendation:

- PBGC should remove FTP from any remaining systems. **(OIG Control Number FISMA-15-04)**

b. Credentialed Scanning

Credentialed scans are granted local access to scan the target system. These authenticated network scans often requires elevated privileges to allow a remote network audit to obtain detailed information such as installed software, missing security patches and operating system settings. These include both external scans carrying a credential or scans by a sensor agent resident on the device, running as a system or as a privileged account.

PBGC's Enterprise Cybersecurity Division began quarterly credential scanning in August 2015, and as of October 2015 PBGC was in the process of harmonizing the scanning activities within the organization.

In FY 2016, PBGC implemented a credentialed scanning program and began a quarterly credentialed scanning program for some of PBGC's general support systems. However, this program did not provide coverage for all of PBGC's general support systems. PBGC is in the process of improving and maturing its credentialed scanning program for its general support systems.

Also, the *FY15 CIO Annual FISMA Metrics* Version 1.2, dated July 30, 2015, asks agencies to provide the percent of hardware assets assessed using credentialed (privileged) scans with Security Content Automation Protocol (SCAP) validated vulnerability tools.

Recommendation:

- Perform scheduled credentialed scans to include all the systems and update PBGC policies and procedures to require regular credentialed scans. **(OIG Control Number FISMA-15-05)**

3. Identity And Access Management

a. Access Control

In FY 2016, PBGC conducted a review of accounts and determined that 4,100 Oracle accounts did not meet its password and account lockout policy. These accounts were created over time and the intended purpose of these accounts is unknown. PBGC is currently in the process of reviewing these accounts to determine if they can be made compliant with its policy *PBGC Identification and Authentication Standard (SE-STD-01-27) and PBGC Access Control Standard (SE-STD- 01-32)*.

Recommendation:

- Complete research on whether 4,100 Oracle service accounts can be made compliant with the new FY 2016 password and lockout standards, while continuing to implement procedures to consistently apply password and account lockout settings for databases. **(OIG Control Number FISMA-16-01)**

b. Account Re-certification

PBGC did not complete the FY 2016 Account Recertification for the Information Technology Infrastructure Services General Support System (ITISGSS) by the August 12, 2016 deadline. The Federal Managers, Contractor Officer Representatives and those identified with authorization to recertify accounts had completed only 50% of the account recertifications as of September 23, 2016.

NIST SP 800-53, Revision 4, under Account Management states that the organization will "create, enable, modify, disable, and remove information system accounts in accordance with [PBGC *User & Access Recertification Process*, Version 7.0]." CLA noted that PBGC has not followed the steps outlined within the PBGC *User & Access Recertification Process*, Version 7.0, as required.

PBGC implemented a new system for automating the account recertification process. However, PBGC did not include adequate time to develop, implement, and complete the recertification process. Office of Information Technology (OIT) recertification due dates for persons with authority to recertify were as late as August 31, 2016, which was 13 business days after the date set by the Enterprise Cybersecurity Division.

Recommendation:

- PBGC should ensure that adequate time is provided to complete the account recertification by the deadline. **(OIG Control Number FISMA-16-02)**

4. Incident Response And Reporting

a. Incident Handling and Security Monitoring

PBGC purchased an automated tool, Splunk, to collect, analyze, search, and monitor information system security logs across the general support system. However, this tool was not fully configured to collect data enterprise-wide and not all information system owners provided a timeline for implementation. The current implementation of the tool has enhanced PBGC's detection of security events; however, PBGC has not implemented this tool for its major applications. PBGC began to collaborate with other departments and system owners to identify application log activity to be ingested into Splunk in FY 2016. When fully implemented across PBGC, the tool will exponentially increase PBGC's capability to detect security events.

In FY 2016, PBGC also began the process to identify business needs and gaps associated with PBGC's current data loss prevention (DLP) program. This gap analysis will serve as the foundation for identifying and implementing more effective controls to protect against data loss.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* states:

> **D.2.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)**
> To enhance the ability to identify inappropriate or unusual activity, organizations may integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information through the use of SIEM tools. SIEM tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components. SIEM tools can also facilitate audit record correlation and analysis. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results.

Recommendations:

- 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 Number FS-07-17) (PBGC revised date: June 30, 2017)**
- 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 Number FS-14-12) (PBGC revised date: June 30, 2017)**

5. Risk Management

a. PBGC's Background Reinvestigation

In FY 2016, we found PBGC still had not implemented an effective background reinvestigation process. We first noted PBGC did not conduct background reinvestigations when employees changed jobs or roles to one in which the position risk designation is assessed at a higher level. In FY 2015, positions at the High and Moderate risk levels were referred to as "Public Trust" positions. Public Trust positions involve access to and operation or control of proprietary systems or information, such as financial and personal records, with a significant risk for causing damage to people, PBGC, or for realizing personal gain. We noted the following weaknesses from a sample of 24 background investigations tested in FY 2016:

- Seven personnel background investigations were not initiated through Office of Personnel Management (OPM) electronic questionnaire for investigations processing (e-QIP) for at least five months after their position changed.
- Six personnel required a new background investigation due to the expiration of their clearance. However, a halt was put on reinvestigations for those users that possessed an expired investigation that sufficed for their needed risk level.
- One person had an expired clearance, and had not begun a new investigation for a higher risk level due to the lag in definition of their position risk level designation. PBGC was not able to finalize the position's risk level designation. The investigation was halted until the position designation is finalized.

During FY 2016, PBGC authorized a halt on background investigations until the OPM guidance was made available for PBGC to re-designate each federal position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. The change was due to the new Title 5 Code of Federal Regulations Part 1400, *Designation of National Security Positions*.

Recommendation:

o 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) (PBGC's Scheduled Completion Date: June 30, 2016)**

b. Security Management

In FY 2015, we found PBGC did not complete the annual security control assessment for one of its major applications and recommended PBGC to evaluate and determine the effectiveness of existing controls to ensure annual security control assessments are completed timely for all major applications and general support systems. As a result, in January 2016, PBGC conducted a root cause analysis and developed a policy road map to identify needed policies and updates to existing policies and procedures to reflect the RMF. The analysis identified the need to update the PBGC Directive IM 05-02, *PBGC IT Security Program*, which was last completed in March 2012. PBGC also needed to transition from its *Security Authorization Guide version 3.1* to PBGC's RMF process.

As part of the transition, PBGC trained Authorizing Officials (AOs), Information System Owners/Information Owners (ISO/IOs), Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs) on the RMF process during role-based training sessions.

To ensure consistency and that the new process is repeatable, PBGC updated in June 2016 the Security and Privacy Assessment & Authorization (SP A&A) pre- and post-assessment checklists to include the review of the Information System Continuous Monitoring Plans. Continuous monitoring is one of six steps in the Risk Management Framework described in NIST Special Publication 800-37, Revision 1, *Applying the Risk Management Framework to Federal Information Systems*. The purpose of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur. The Continuous Monitoring Plan provides oversight and monitoring of the

security controls in the information system on an ongoing basis.
Additionally, the ***FY15 Annual Enterprise Continuous Monitoring (ECM) Plan*** states:

> The PBGC Enterprise Continuous Monitoring Plan documents the Enterprise Continuous Monitoring Control Selection Methodology and Monitoring Frequency for identifying the subset of NIST 800-53, Rev. 4 controls that all PBGC departments must assess to determine the control's operating effectiveness. The results of the assessment are required to be documented in Cyber Security Assessment and Management (CSAM).

Recommendation:

- Evaluate existing controls and determine effectiveness to ensure annual security control assessments are timely completed for all major applications and general support systems. **(OIG Control Number FISMA-15-07) (PBGC's Scheduled Completion Date: June 30, 2017)**

c. Ongoing Authorization

After review of requirements for systems authorizations and ongoing authorization, we noted PBGC has systems in ongoing authorization without the correct, finalized, and up-to-date security documentation recorded in the required CSAM container "Status and Archive", as required by PBGC policy. Specifically, these security documents are required to be uploaded in the CSAM repository tool anytime a change is made or a document is created. CSAM is PBGC's official and authoritative repository for system authorizations. The security documents support the initial authorization, reauthorization, and ongoing authorization reviews of PBGC's systems. Required documentation are maintained in CSAM as artifacts to support the system was authorized in accordance with the RMF. Security documentation is stored in CSAM on the categorization, selection, implementation, and assessment of controls, system authorization, and monitoring.

The Corporate Performance System (CPS) did not contain the following documents within the CSAM repository:

- The Plan of Action and Milestones (POA&M) Report and Security Assessment Report (SAR) for ongoing authorization were not included in CSAM "Status and Archive" container. PBGC communicated that these documents did not have to be loaded into CSAM because CSAM is able to generate the POA&M and SAR. However, PBGC was not able to confirm if CSAM is able to generate a report for a point in time. In addition, the Authorizing Official is responsible for retaining the authorization package. However, PBGC policy does not provide the retention timeframe.

The Consolidated Financial System (CFS) did not contain the following documents within the CSAM repository:

- The Classification and Determination Memo (C&DM), Federal Information Processing Standards (FIPS) 199, Privacy Threshold Analysis (PTA), and POA&M report.

The Electronic Complaints and Tracking System (eCATS) did not contain the following documents within the CSAM repository:

- CSAM "Status and Archive" container was not linked to the System of Records Notice (SORN). PBGC communicated the SORN was in CSAM; however, it was not linked to the SORN field in the "Status and Archive" container for that system. While it is in the

CSAM application, the document is not referenced from the correct place.

The Enterprise Cybersecurity Division (ECD) did not review the “Status and Archive” folder consistently for all systems as information is not consistently maintained in the folder. ECD checks the “Status and Archive” container as part of their post assessment review of the security assessment and authorization documentation. However, the “Status and Archive” container did not always contain the necessary historical information for review as noted above.

CLA has noted that the Security and Privacy Assessment and Authorization (SPA&A) Review Checklist requires ECD and the Privacy Office to assess all of the artifacts and material in CSAM. However, the checklist did not require the reviewer to confirm that the ongoing authorization documentation was in the “Status and Archive” container. For example, the checklist requires the reviewer to confirm only that the SAR was aligned to the Security Assessment Plan (SAP), all applicable controls were assessed, and appropriate evidence supported the control assessments.

The *PBGC Information Security Risk Management Framework Process* is not clear on the requirements for maintaining the SAR, POA&M, and Authorization to Operate (ATO) package in the “Status and Archive” container in CSAM.

Recommendations:

- Implement quarterly reviews of the “Status and Archive” to verify system authorization artifacts and information are stored within CSAM. **(OIG Control Number FISMA-16-03)**

- Update PBGC policy to clarify the requirements for maintaining the POA&M and SAR generated for the authorization to operate package. **(OIG Control Number FISMA-16-04)**

- Update the RMF Process to clearly state where system security documentation and artifacts are required to be loaded into CSAM. **(OIG Control Number FISMA-16-05)**

d. Organization Risk Tolerance

PBGC had not made a determination of its organizational risk tolerance. PBGC’s acting Risk Management Officer decided to let the permanent Risk Management Officer determine PBGC’s organizational risk tolerance. PBGC has not selected and/or appointed the permanent Risk Management Officer.

NIST SP 800-53, Revision 4, PM-9 Risk Management Strategy requires the organization “to develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems.” Further requirements include the implementation, review and the updating of the risk management strategy consistently across the organization.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, states “the objective of establishing an organizational risk tolerance is to state in clear and unambiguous terms, a limit for risk — that is, how far organizations are willing to go with regard to accepting risk to organizational operations (including missions, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation.”

Recommendation:

- o PBGC should establish its organizational risk tolerance and integrate all organizational processes, procedures, and risks with this risk tolerance. **(OIG Control Number FISMA-16-06)**

e. Risk Assessment

PBGC was not in compliance with its *Risk Assessment Standard* (SE-STD-01-14) updated September 12, 2013, which requires the annual review of risk assessment results. In FY 2016, PBGC did not review the risk assessment results for ITISGSS. We noted that the risk assessment was not reviewed or updated. Changes in threats and security requirements were not assessed, and strategies for mitigating additional risks were not updated and/or developed.

In addition, the RMF process did not include a requirement to annually review or conduct a risk assessment. Currently, the RMF requires an initial risk assessment to determine if additional controls should be selected and is to be re-completed to identify any changes to the system's operating environment that may drive changes to the ISCM plan.

Recommendations:

- o PBGC should ensure adequate staffing for the annual review of major applications and general support systems risk assessments. **(OIG Control Number FISMA-16-07)**

- o Update the *Information Security Risk Management Framework Process* to refer to the Cybersecurity and Privacy Catalog (CPC) for the requirements for a risk assessment. **(OIG Control Number FISMA-16-08)**

f. New Hire Process

CLA noted four out of nine federal employees did not complete Form I-9, *Employment Eligibility Verification.* From a sample of 25 out of 552 new federal employees and contractors, from October 1, 2015 through May 31, 2016, CLA noted that 9 of the 25 personnel sampled were federal employees.

PBGC Directive Personnel Management (PM) 05-01, *PBGC Entrance on Duty and Separation Procedures for Federal and Contract Employees*, requires all contractors and federal employees upon entrance of duty to complete the I-9, *Employment Eligibility Verification* form.

Recommendation:

- o PBGC should develop and implement a secondary review process between the Human Resource Department and Workplace Solutions Department (WSD) to ensure completion of Form I-9, *Employment Eligibility Verification.* **(OIG Control Number FISMA-16-09)**

g. Separation Process and Inactive Accounts

CLA noted the following weaknesses in the sample of 25 separated and transferred personnel:

i. PBGC forms for the separation clearance for federal and contractor employees were:
   - Incomplete for 13 of the 25 personnel sampled.

- Not completed on or before the last official day with PBGC for 13 of 25 personnel sampled.
- Not provided for 2 of the 25 personnel sampled.

ii. An OIT User Asset Report was not provided for 10 of the 25 personnel sampled.

iii. GetIT Ticket requests were made from 2 to 44 days after the separation date for 21 of the 25 personnel sampled.

CLA noted the following observations upon comparing the active Case Management System (CMS) users to the separated user report:

Nine separated users remained on the CMS system generated report of active users.

- Nine accounts for separated employees within the Active Directory were disabled, but five of nine accounts were not removed from CMS.
    - One of the five CMS accounts remained on an orphan queue for five months until the separation request was finally addressed.
    - Four of five CMS accounts were removed from Active Directory, but remained on the CMS Active User report.
- Four of nine CMS accounts were removed after separation date.

CLA noted the following weaknesses during review of Active TeamConnect Users:

Per discussion with management, inactive accounts will not be deactivated by the system until the user attempts to login.

- One user had not logged into TeamConnect since their account creation date of November 3, 2015.
- One user retained an active TeamConnect account despite a last login date of August 27, 2012.

Per review of the *PBGC Physical and Personnel Security Process Manual,* version 2.0, dated May 19, 2015, section 4.1 indicates that the Personnel Security Team (PST) will review the PBGC Separation Form 169/C to validate completion of all required signatures, dates and initials.

The WSD Security section listed under the Separation Clearance PBGC Connect intranet page states that the PBGC Form 169/C is to be submitted on or before the separating employee's last official day to WSD Security complete with ALL signatures. User Asset Reports are also to be submitted along with the PBGC Form 169C.

WSD Security Forms for federal employees and contractors indicate that GetIT system separation requests are to be submitted on or before the federal/contractor employee's last official day.

CLA reviewed the ITIO Work Instruction: *Active Directory Dormant Account Process*, version 1.3, dated June 22, 2016, and noted that the Deletion of Accounts, under Section 2 *Dormant Account Process*, indicates that accounts are to be de-provisioned after 90/365 days of inactivity.

Recommendations:

- o PBGC should enhance the review process to ensure the completion of the PBGC Separation Form 169/C and annotate when completion is not required. **(OIG Control Number FISMA-16-10)**

- o PBGC should provide training to Federal Managers and CORs to ensure adherence to PBGC policy during the separation process for timely completion of the Separation Form 169/C and initiation of separation requests in the GetIT system. **(OIG Control Number FISMA-16-11)**

- o PBGC should enhance the process for removing separated and inactive accounts to include applications, not just Active Directory. **(OIG Control Number FISMA-16-12)**

6. Security Training

a. Security Awareness Training

CLA noted that there was a total population of 2,276 user owned Active Directory accounts. We noted the following weaknesses in PBGC's security awareness training program:

i. We compared this population to the list of users that completed the annual security awareness training. We noted that there were 377 users in Active Directory that had not completed training by the June 30, 2016 due date.

ii. From this subset of 377 users, a sample of 25 users was selected. Of the 25 users, we noted the following regarding 13 users after consultation with PBGC:
   - Eight users did not have a Talent Management System (TMS) account at the time of training, and therefore did not complete training.
     - o One user had a TMS account created after the June 30, 2016 due date.
   - Four users had a TMS account and did not complete training.
   - One user had a TMS account, but separated before the June 30, 2016 due date.

NIST SP 800-53, Rev. 4, *AT-2 Security Awareness Training,* indicates that the organization is responsible for providing basic security awareness training to information system users.

Under PBGC *Security Awareness and Training Procedure*s Version 1.1, *Security Awareness and Training Mandate* 1, "annually and as needed," PBGC will provide all staff with basic security awareness and training.

Recommendation:

- o PBGC should develop and implement process and procedures and require all users with access to PBGC systems or information complete security awareness training. **(OIG Control Number FISMA-16-13)**

b. Role-based Training

PBGC did not ensure that all personnel with significant IT security responsibilities completed the required role-based training in FY 2015. After performing a root cause analysis, PBGC established a POA&M to ensure the proper implementation and resolution of the conditions noted. In an effort to enhance the current program, efforts were taken to improve the management of its current records to ensure those individuals identified with security responsibilities receive the required training. PBGC has identified all personnel with significant IT security responsibilities and has communicated to them required training. Some milestones established in the POA&M have been completed to address the role-based training process.

The PBGC Directive IM 05-2, PBGC Information Security Policy required the following:

i. General security awareness training shall be provided periodically to all users.
ii. Role-based annual training shall be provided to those users with substantial security responsibilities.

Recommendation:

o PBGC should increase records management controls and monitoring to ensure all required personnel timely complete role-based training. **(OIG Control Number FISMA-15-08) (PBGC's Scheduled Completion Date: December 31, 2016)**

c. Insider Threat

PBGC has not implemented an insider threat detection and prevention program.

PBGC has not created a cross-discipline insider threat incident handling team, or assigned a senior organizational official to be the responsible individual to implement and provide oversight for the program.

NIST SP 800-53, Rev. 4, PM-12, *Insider Threat Program*, indicates that the organization is required to implement an insider threat program that includes a cross-discipline insider threat incident handling team.

Recommendation:

o PBGC should assign a senior organizational official, and develop and implement an insider threat detection and prevention program. **(OIG Control Number FISMA-16-14)**

7. Contingency Planning

In FY 2016, CLA conducted a site visit to PBGC's paying agent. The paying agent owns the PLUS Program. The PLUS Program is to provide pension and lump sum payments to pension plan participants. Contingency planning was part of our testing at the paying agent. NIST SP 800-34, Revision 1*, Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods."

a. PBGC's Business Impact Analysis

PBGC indicated that its Business Impact Analysis (BIA) was not conducted in accordance with NIST 800-34 Revision 1, but based on Federal Continuity Directive 1 (FCD1) *Federal Executive Branch National Continuity Program and Requirements* and Federal Continuity Directive 2, *Federal Executive Branch Mission Essential Functions and Candidate Primary Mission Essential Functions Identification and Submission Process*. PBGC is in the process of updating its BIA. However, there is no indication that PBGC will prepare a BIA in accordance with NIST guidance, as required by FISMA of 2014.

Officials stated that the PBGC BIA is dictated by business function, as identified by business owners, and the BIA was created as required by the Federal Continuity Directive, not NIST SP 800-34. The PBGC BIA does not define system requirements, so the rating in PBGC's BIA would have no effect on the PLUS COOP requirements. Furthermore, the PLUS system owner and Information System Security Officer indicated that they were not aware of the existence of PBGC's 2012 BIA and did not consider it in establishing recovery times for PLUS.

b. CSAM

PBGC indicated that definitions and rating of the system's availability in CSAM are system specific and not uniform for all systems. Information produced in CSAM dashboards cannot provide PBGC officials with perspective and oversight, as the amalgamation of results mixes ratings for each system based on differing definitions.

c. PLUS Business Impact Analysis

The PLUS Business Impact Analysis provided for review did not meet NIST Special Publication 800-34, Rev. 1 *Contingency Planning Guide for Federal Information Systems.* PBGC provided 7 BIAs for the PLUS system; none of them complied with the NIST 800-34, Rev. 1 definition of BIA.

d. FIPS 199 Categorization

PBGC's FIPS 199 Categorization of PLUS is inconsistent. We noted the following inconsistencies in CSAM and PLUS documentation:

i. System Availability for PLUS is documented as "moderate" in the PLUS System Information Type obtained from CSAM.

ii. The FIPS 199 System Security Categorization of PLUS categorizes PLUS as "low."

- The FIPS 199 System Security Categorization of PLUS states that the provisional impact level is "moderate" and the final impact level is "low." Per PBGC management, any difference in categorization would require justification. However, the justification provided did not explain the method and reasoning for system availability to be "low."

iii. The PLUS System Security Plan (SSP) categorizes PLUS as "low" for availability.

e. PLUS ISCM

The FY 2017 PLUS Information Security Continuous Monitoring Plan (ISCM) states that PLUS is a High Value Asset (HVA) which was determined by the HVA Privacy and Security Review performed by ECD and the Privacy Office on March 17, 2016. However, PLUS is still considered "low" for availability by the owners of PLUS.

f. PBGC's COOP

PBGC's Annual COOP Exercise Test Plan lists PLUS' recovery timeframe to be eight days. The COOP does not consider PLUS as a "low availability" system. Low availability systems are not tested as part of PBGC's COOP test.

g. PLUS Recovery Time

The PLUS SSP states that the paying agent restores PLUS within 48 hours. The PLUS SSP Appendix D: Control Report states the PLUS Recovery Time Objective (RTO) is 24 hours and its supporting components have an RTO of 48 hours. The RTO contradicts the categorization of "low" availability noted in the PLUS SSP.

h. Continuity of Operations Plan Test Results

The Office of Benefits Administration (OBA) participated in PBGC's annual COOP test between February 5, 2016 and February 6, 2016. Moreover, file transfers from PBGC's disaster recovery site located in Wilmington, DE and the PLUS backup server located in Jacksonville, FL were not tested. The Risk Acceptance for Contingency Planning of PLUS states that the paying agent's Contingency Plan test does not include testing of the backup file transfer component or operations, but file transfers are tested as part of the PBGC COOP test. The risk of the paying agent not testing backup files as part of their Disaster Recovery test was accepted with reliance that the backup file transfers are tested during the PBGC COOP test. However, the compensating measure was not in place during the PBGC's annual COOP test. In addition, the PLUS Authorizing Official was not informed of the lack of COOP testing and the impact to the Risk Acceptance.

NIST SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems* states that the BIA is a key step in implementing the Contingency Planning controls outlined within 800-53. By accomplishing the BIA PBGC will: determine mission/business processes and recovery criticality, identify resource requirements and identify recovery priorities for system resources.

PBGC published its BIA in 2012, but was unable to communicate the BIA results to all stakeholders. Security documents were not reviewed to ensure consistency and as a result security definitions were not uniform or consistent between its systems and documents.

In FY 2016, PBGC's COOP test and test results had reporting errors, which were not clearly communicated to stakeholders. PBGC is unable to communicate policy and security determination to all stakeholders as there is no effective policy in place to do so.

Recommendations:

- As required by FISMA, PBGC should complete a Business Impact Analysis (BIA) in accordance with NIST guidance. **(OIG Control Number FISMA-16-15)**

- PBGC should use its BIA in determining the categorization and recovery time objective of the PLUS application. **(OIG Control Number FISMA-16-16)**

- PBGC should ensure that security definitions across its systems and documentation are consistent. **(OIG Control Number FISMA-16-17)**

- PBGC should ensure that security documentation do not contradict each other and are consistent with its policy. **(OIG Control Number FISMA-16-18)**

- PBGC should develop and implement processes and procedures for effective communication of its security policies and processes. **(OIG Control Number FISMA-16-19)**

- PBGC should improve its process of communicating COOP test plans and test results to ensure errors in documentation is eliminated for effective reporting to its stakeholders. **(OIG Control Number FISMA-16-20)**

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 2016 and 2015 Financial Statements Audit* (*AUD 2017-3/FA-16-110-2)*, issued November 15, 2016).

Finding Summary	Recommendations
1. Entity-Wide Security Program Planning and Management While PBGC continued to make progress in addressing the Corporation's entity-wide security program planning and management control deficiencies, these efforts have not resulted in a fully implemented effective entity-wide information security program as required under OMB and the National Institute of Standards and Technology (NIST) guidance. These requirements provide a framework for assessing and managing risk, including developing and implementing security policies and procedures, conducting security awareness training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of the Corporation's sensitive or critical resources. We note the following progress by management in this area. In FY 2016, PBGC developed and published the PBGC Risk Management Framework (RMF) process to transition and fully implement an entity-wide information security risk management program. PBGC's IT risk management focuses on identifying and evaluating the threats and opportunities pertinent to the proposed IT program/project and identifying risk management and mitigation strategies. The RMF will address both security and privacy controls when fully implemented. PBGC is proactive in addressing new federal guidance on IT security and privacy and developing	• Complete the PBGC RMF transition, fully implement the entity-wide information security risk management program and provide periodic updates to stakeholders. **(OIG Control Number FS-15-02) (PBGC completion date:** PBGC submitted corrective action completion documentation after audit fieldwork completed. OIG will assess the corrective action submission during the FY 2017 FISMA audit cycle.**)** • Complete the migration to NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* and provide periodic updates to stakeholders. **(OIG Control Number FS-15-03) (PBGC completion date:** PBGC submitted corrective action completion documentation after audit fieldwork completed. OIG will assess the corrective action submission during the FY 2017 FISMA audit cycle.**)** • Complete the implementation of NIST SP 800-53, Revision 4 controls for common controls, remediation of common controls weaknesses and make available to system owners in Cyber Security Assessment and Management for appropriate inclusion in their system security plans. **(OIG Control Number FS-15-04) (PBGC completion date:** PBGC submitted corrective action completion documentation after audit fieldwork completed. OIG will assess the corrective action submission during the FY 2017 FISMA audit cycle.**)**

Finding Summary	Recommendations
corrective actions to address potential control gaps. In addition, PBGC has developed and is implementing a plan to be fully compliant with OMB Circular A-130, *Managing Information as a Strategic Resource,* issued on July 28, 2016. PBGC, however, has not fully implemented components of its entity-wide information security risk management program. Some components not fully implemented include the following: • Completion of the implementation of PBGC's-wide security program and management, which supports PBGC organizational, mission and information system objectives by addressing each of the six RMF phases: categorize, select, implement, assess, authorize, and monitor. • Full implementation of a continuous monitoring program. • Common control compliance with NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations r*equirements. • Completion of the transition to NIST 800-53, Revision 4 security controls. • Full Implementation of common controls and remediation of common control weaknesses. • Availability of common controls to system owners for appropriate inclusion in system security plans. PBGC implementation of NIST's RMF will establish an integrated enterprise-wide decision structure for cybersecurity risk management that includes and integrates PBGC mission and information system objectives, which will transition to near real-time risk management. This Framework will also address common controls weaknesses and full implementation of continuous monitoring controls. The Corporation had established a timeline for transition to the RMF requirements by September 2016. The Enterprise Cybersecurity Division Monthly update for November 2015 identified that the NIST	

Finding Summary	Recommendations
800-53, Revision 4 controls transition should be completed by January 29, 2016. As of August 30, 2016, 43% of enterprise common controls (ECCs) have been implemented. The Information Technology Infrastructure Operations Department (ITIOD) owns 153 of the ECCs, of which 16% have been implemented.	
2. Access Controls and Configuration Management While PBGC made progress in addressing access controls and configuration management deficiencies identified in previous years, this progress did not fully resolve some security weaknesses. Weaknesses in the PBGC IT environment continue to contribute to deficiencies in system configuration, segregation of duties and role-based access controls based on least privilege. In FY 2016, PBGC continued to implement various tools and processes to establish a more coherent environment for access controls and configuration management security controls. PBGC, however, pushed out the dates for many planned corrective actions by one year or more. We continue to make the recommendations noted below to address the underlying access controls and configuration management weaknesses in PBGC's information system security controls. The controls not fully implemented include the following: • Implementation of controls to remedy vulnerabilities identified in key databases and applications, such as weaknesses in configuration, roles, privileges, auditing, file permission and operating system access. • Development and implementation of processes and procedures for determining and documenting defined security configuration checklists for database applications. • Implementation of requirements for the disposition of dormant accounts for all	• 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 Number FS-07-14) (PBGC revised completion date: June 30, 2018)** • 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 IAH). **(OIG Control Number FS-07-12) (Closed as of November 30, 2016)** • Continue to remove unnecessary user and generic accounts. **(OIG Control Number FS-07-08) (PBGC revised completion date: to be determined*)** • Fully implement controls to plan, remove and decommission unsupported systems and databases. **(OIG Control Number FS-16-07) (PBGC's Scheduled Completion Date: June 30, 2018)** • Develop and implement plan of action for addressing known security weaknesses. **(OIG Control Number FS-16-08) (PBGC's Scheduled Completion Date: June 30, 2017)**

Finding Summary	Recommendations
PBGC systems. - Full implementation of controls to remove separated users from systems and applications. - Removal and decommission of systems and databases that have reached their end of service life. - Development and implementation of a plan of action to address known security weaknesses in accordance with PBGC's timeline for corrective actions. 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. An information system is comprised of many components[1] that can be interconnected in a multitude of arrangements to meet a variety of business, mission and information security needs. How these information system components are networked, configured and managed is critical in providing adequate information security and supporting an organization's risk management process.	

* 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.

[1] Information system components include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, Web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

VIII. FISMA RECOMMENDATIONS CLOSED IN FISCAL YEAR 2016

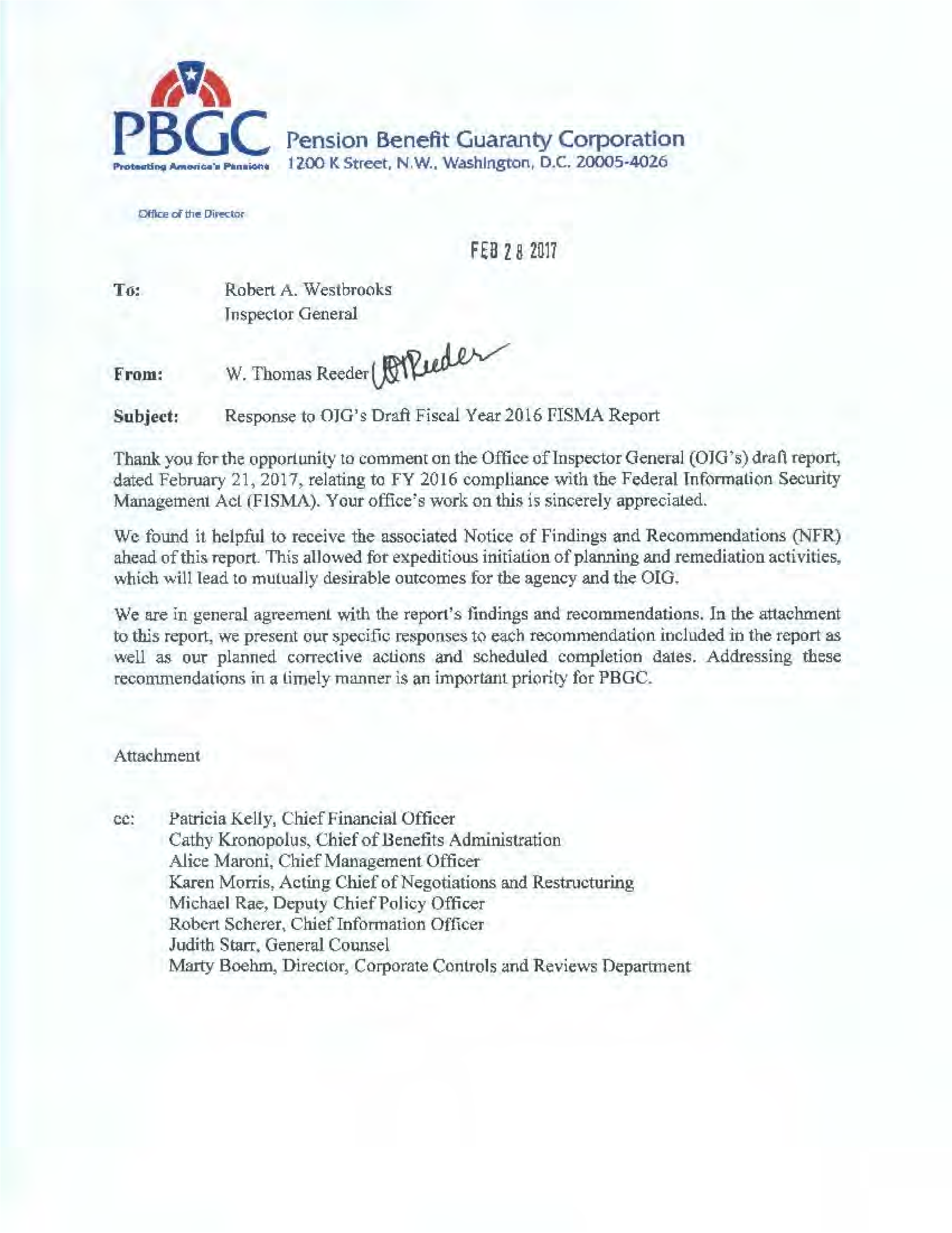
OIG Control Number	Date Closed	Original Report Number
FISMA-11-02	December 6, 2016	EVAL-2012-9/FA-11-82-7
FISMA-13-15	September 29, 2016	EVAL-2014-9/FA-13-93-7
FISMA-13-17	October 25, 2016	EVAL-2014-9/FA-13-93-7
FISMA-13-18	October 25, 2016	EVAL-2014-9/FA-13-93-7
FISMA-14-01	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-02	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-03	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-04	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-05	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-11	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-12	March 31, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-19	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-14-20	November 30, 2016	EVAL 2015-9/FA-14-101-7
FISMA-15-06	September 29, 2016	FA-15-108-7/EVAL 2016-7
FS-14-09	February 14, 2017	AUD-2015-3/FA-14-101-3
FS-14-10	February 14, 2017	AUD-2015-3/FA-14-101-3

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

OIG Control Number	Original Report Number
Prior Year	
FISMA-14-15	EVAL 2015-9/FA-14-101-7
FISMA-15-01	(FA-15-108-7/EVAL 2016-7)
FISMA-15-02	(FA-15-108-7/EVAL 2016-7)
FISMA-15-03	(FA-15-108-7/EVAL 2016-7)
FISMA-15-04	(FA-15-108-7/EVAL 2016-7)
FISMA-15-05	(FA-15-108-7/EVAL 2016-7)
FISMA-15-07	(FA-15-108-7/EVAL 2016-7)
FISMA-15-08	(FA-15-108-7/EVAL 2016-7)
FS-07-17	AUD-2009-3/FA-08-49-3
FS-14-12	AUD-2015-3/FA-14-101-3
Current Year	
FISMA-16-01	EVAL 2017-9 /FA-16-110-7
FISMA-16-02	EVAL 2017-9 /FA-16-110-7
FISMA-16-03	EVAL 2017-9 /FA-16-110-7
FISMA-16-04	EVAL 2017-9 /FA-16-110-7
FISMA-16-05	EVAL 2017-9 /FA-16-110-7
FISMA-16-06	EVAL 2017-9 /FA-16-110-7
FISMA-16-07	EVAL 2017-9 /FA-16-110-7
FISMA-16-08	EVAL 2017-9 /FA-16-110-7
FISMA-16-09	EVAL 2017-9 /FA-16-110-7

OIG Control Number	Original Report Number
FISMA-16-10	EVAL 2017-9 /FA-16-110-7
FISMA-16-11	EVAL 2017-9 /FA-16-110-7
FISMA-16-12	EVAL 2017-9 /FA-16-110-7
FISMA-16-13	EVAL 2017-9 /FA-16-110-7
FISMA-16-14	EVAL 2017-9 /FA-16-110-7
FISMA-16-15	EVAL 2017-9 /FA-16-110-7
FISMA-16-16	EVAL 2017-9 /FA-16-110-7
FISMA-16-17	EVAL 2017-9 /FA-16-110-7
FISMA-16-18	EVAL 2017-9 /FA-16-110-7
FISMA-16-19	EVAL 2017-9 /FA-16-110-7
FISMA-16-20	EVAL 2017-9 /FA-16-110-7

X. MANAGEMENT’S RESPONSE



PBGC
Protecting America's Pensions

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

Office of the Director

FEB 28 2017

To: Robert A. Westbrooks
Inspector General

From: W. Thomas Reeder Reeder

Subject: Response to OIG’s Draft Fiscal Year 2016 FISMA Report

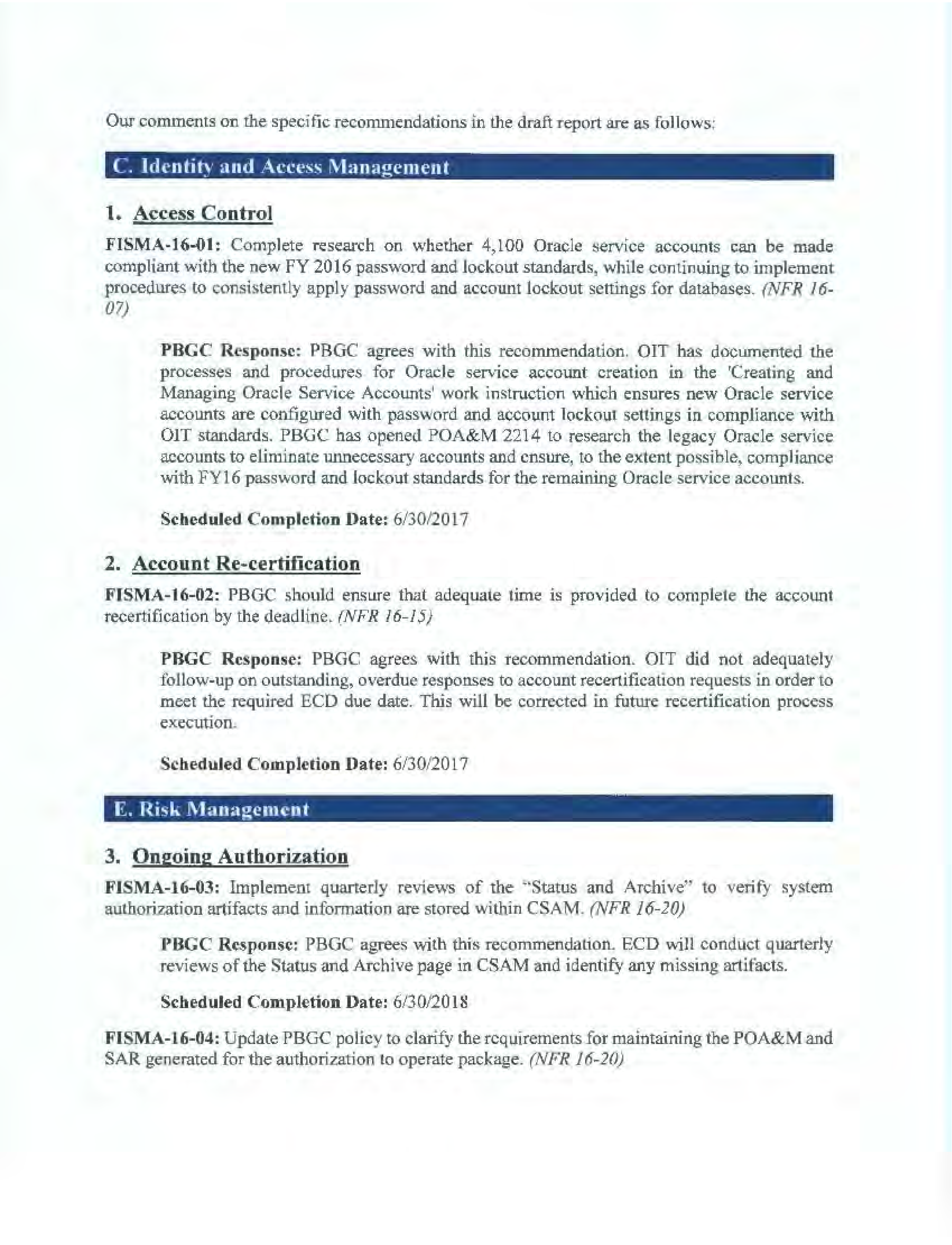
Thank you for the opportunity to comment on the Office of Inspector General (OIG’s) draft report, dated February 21, 2017, relating to FY 2016 compliance with the Federal Information Security Management Act (FISMA). Your office’s work on this is sincerely appreciated.

We found it helpful to receive the associated Notice of Findings and Recommendations (NFR) ahead of this report. This allowed for expeditious initiation of planning and remediation activities, which will lead to mutually desirable outcomes for the agency and the OIG.

We are in general agreement with the report’s findings and recommendations. In the attachment to this report, we present our specific responses to each recommendation included in the report as well as our planned corrective actions and scheduled completion dates. Addressing these recommendations in a timely manner is an important priority for PBGC.

Attachment

cc: Patricia Kelly, Chief Financial Officer
Cathy Kronopolus, Chief of Benefits Administration
Alice Maroni, Chief Management Officer
Karen Morris, Acting Chief of Negotiations and Restructuring
Michael Rae, Deputy Chief Policy Officer
Robert Scherer, Chief Information Officer
Judith Starr, General Counsel
Marty Boehm, Director, Corporate Controls and Reviews Department



Our comments on the specific recommendations in the draft report are as follows:

C. Identity and Access Management

1. Access Control

FISMA-16-01: Complete research on whether 4,100 Oracle service accounts can be made compliant with the new FY 2016 password and lockout standards, while continuing to implement procedures to consistently apply password and account lockout settings for databases. *(NFR 16-07)*

> **PBGC Response:** PBGC agrees with this recommendation. OIT has documented the processes and procedures for Oracle service account creation in the 'Creating and Managing Oracle Service Accounts' work instruction which ensures new Oracle service accounts are configured with password and account lockout settings in compliance with OIT standards. PBGC has opened POA&M 2214 to research the legacy Oracle service accounts to eliminate unnecessary accounts and ensure, to the extent possible, compliance with FY16 password and lockout standards for the remaining Oracle service accounts.
>
> **Scheduled Completion Date:** 6/30/2017

2. Account Re-certification

FISMA-16-02: PBGC should ensure that adequate time is provided to complete the account recertification by the deadline. *(NFR 16-15)*

> **PBGC Response:** PBGC agrees with this recommendation. OIT did not adequately follow-up on outstanding, overdue responses to account recertification requests in order to meet the required ECD due date. This will be corrected in future recertification process execution.
>
> **Scheduled Completion Date:** 6/30/2017

E. Risk Management

3. Ongoing Authorization

FISMA-16-03: Implement quarterly reviews of the "Status and Archive" to verify system authorization artifacts and information are stored within CSAM. *(NFR 16-20)*

> **PBGC Response:** PBGC agrees with this recommendation. ECD will conduct quarterly reviews of the Status and Archive page in CSAM and identify any missing artifacts.
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-04: Update PBGC policy to clarify the requirements for maintaining the POA&M and SAR generated for the authorization to operate package. *(NFR 16-20)*

PBGC Response: PBGC agrees with the recommendation. The PBGC RMF Process should be clarified to explain when it is appropriate to use the Report and the SAR Report fields on the Status and Archive page. These updates to the process will be made during the annual review of the document in 2017.

Scheduled Completion Date: 6/30/2018

FISMA-16-05: Update the RMF Process to clearly state where system security documentation and artifacts are required to be loaded into CSAM. *(NFR 16-20)*

PBGC Response: PBGC agrees with this recommendation. The PBGC RMF Process should be clarified to add the location where required artifacts should be uploaded into CSAM. These updates to the process will be made during the annual review of the document in 2017.

Scheduled Completion Date: 6/30/2018

4. Organization Risk Tolerance

FISMA-16-06: PBGC should establish its organizational risk tolerance and integrate all organizational processes, procedures, and risks with this risk tolerance. *(NFR 16-21)*

PBGC Response: PBGC agrees with this recommendation. Consistent with the recent OMB Circular A-123 revision and the requirements of ERISA, as amended by MAP-21, in FY 2016 PBGC appointed an Acting Risk Management Officer, began a search for a permanent Risk Management Officer and established its Risk Management Council (RMC). The RMC has set forth a timetable for the tasks required to implement ERM throughout PBGC, and PBGC has, subsequent to FY-end 2016, completed the process of hiring a permanent Risk Management Officer (RMO). PBGC is also underway with an effort to comply with the NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System view guidance.

As we continue to develop our ERM program, the development of organizational risk tolerances is a priority for the permanent RMO and is incorporated within the current implementation task list established by the RMC. PBGC has already developed organizational risk tolerances for certain components, including OIT. The Risk Management Council (RMC) is currently developing guidance to assist other areas of PBGC in documenting programmatic and operational risk tolerances and other risk inputs. This information will be used as part of the development and integration of the corporate risk profile which must be documented by June 2, 2017 under the revised OMB Circular A-123. The ERM implementation will be appropriately integrated with our existing IT risk management initiatives and will further enhance our compliance with existing NIST 800-53 (PM-9) and NIST 800-37 (RMF) requirements.

As planned, the newly hired Risk Management Officer, Nicole Puri, will provide oversight to ensure completion of the organizational risk profile, and risk tolerances in accordance with PBGC's risk appetite by July 2017.

Scheduled Completion Date: 7/31/2017

5. Risk Assessment

FISMA-16-07: PBGC should ensure adequate staffing for the annual review of major applications and general support systems risk assessments. *(NFR 16-22)*

> **PBGC Response:** PBGC agrees with this recommendation. ITIOD agrees and is working toward reaching a state where the ITISGSS undergoes at least one risk assessment annually. The ITISGSS will achieve this under FY17 by moving from the three-year cycle of performing SA&As to that of Ongoing Authorization (OA).
>
> **Scheduled Completion Date:** 6/30/2017

FISMA-16-08: Update the *Information Security Risk Management Framework Process* to refer to the Cybersecurity and Privacy Catalog (CPC) for the requirements for a risk assessment. *(NFR 16-22)*

> **PBGC Response:** PBGC agrees with this recommendation. ECD's Cybersecurity and Privacy Catalog (CPC) requires Information System Owners to perform a review of the risk assessment at least annually. However, this document was not published until August 2016, which was after the audit work had begun. The *Information Security Risk Management Framework Process* review cycle will be completed before the end of calendar year 2017.
>
> **Scheduled Completion Date:** 12/31/2017

6. New Hire Process

FISMA-16-09: PBGC should develop and implement a secondary review process between the Human Resource Department and Workplace Solutions Department (WSD) to ensure completion of Form I-9, *Employment Eligibility Verification. (NFR 16-06)*

> **PBGC Response:** PBGC agrees with this recommendation. HRD/WSD established an electronic second level review process to ensure completion of the Form I-9, which includes a bi-weekly system reconciliation. The new process was effective December 2, 2016.
>
> **Scheduled Completion Date:** 6/30/2017

7. Separation Process and Inactive Accounts

FISMA-16-10: PBGC should enhance the review process to ensure the completion of the PBGC Separation Form 169/C and annotate when completion is not required. *(NFR 16-10)*

> **PBGC Response:** PBGC agrees with this recommendation. WSD, HRD, and QMD have plans in FY17 to enhance the existing separation process by combining the existing manual, paper-based process involving the PBGC separation forms (169/169C) with the

existing logical access separation process and improving monitoring of separation tickets. These actions will provide PBGC with a more mature separation process with more consistent and timely disposition of PBGC separations.

Scheduled Completion Date: 6/30/2018

FISMA-16-11: PBGC should provide training to Federal Managers and CORs to ensure adherence to PBGC policy during the separation process for timely completion of the Separation Form 169/C and initiation of separation requests in the GetIT system. *(NFR 16-10)*

PBGC Response: PBGC agrees with this recommendation. WSD Security understands the need to provide training to Federal Managers and CORs to ensure adherence to PBGC policy, and will provide training on the new separation process once it has been developed.

Scheduled Completion Date: 6/30/2018

FISMA-16-12: PBGC should enhance the process for removing separated and inactive accounts to include applications, not just Active Directory. *(NFR 16-10)*

PBGC Response: PBGC agrees with this recommendation. PBGC will work to ensure that inactive accounts associated with separated employees are removed from PBGC applications.

Scheduled Completion Date: 6/30/2018

F. Security Training

1. Security Awareness Training

FISMA-16-13: PBGC should develop and implement process and procedures and require all users with access to PBGC systems or information complete security awareness training. *(NFR 16-13)*

PBGC Response: PBGC agrees with NFR 16-13 recommendation but also notes this recommendation is similar to NFR 15-15 (OIG Control Number FISMA 15-08), which was issued in the FY2015 audit and agreed to by PBGC in the management response. PBGC submitted a Progress Status Report (PSR) for NFR 15-15 on 7/28/2016.

In order to mitigate the deficiencies identified in NFR 16-13, PBGC will review the technical aspects of its user provisioning and deprovisioning processes and identify technical solutions to ensure Active Directory and TMS are synchronized. Predicated on a centralized technical solution, PBGC will also develop supplementing controls to ensure all required personnel complete required cybersecurity training.

As PBGC mitigates the deficiencies identified in NFR 16-13, PBGC respectfully requests an administrative closure of FISMA 15-08.

Scheduled Completion Date: 6/30/2017

3. Insider Threat

FISMA-16-14: PBGC should assign a senior organizational official, and develop and implement an insider threat detection and prevention program. *(NFR 16-11)*

> **PBGC Response:** PBGC largely agrees with the recommendation. While NIST SP 800-53 Rev 4, PM-12, Insider Threat Program, suggests implementation of an insider threat program that includes a cross-discipline insider threat incident handling team, the supplemental guidance stipulates that only organizations handling classified information are required, under Executive Order 13587 and the National Policy on Insider Threat, to establish insider threat programs. The same section indicates that standards and guidelines that apply to insider threat programs in classified environments can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems. PBGC will follow the NIST recommendation to leverage existing Security Incident Management (SIM) program and augment it by partnering with other stakeholders in the insider threat efforts (i.e. Workspace Solutions Department, Human Resources Department, Office of General Counsel) to develop a cross-discipline insider threat incident training. A senior official will be responsible for implementation and oversight of the program.
>
> **Scheduled Completion Date:** 6/30/2018

G. Contingency Planning

8. Continuity of Operations Plan Test Results

FISMA-16-15: As required by FISMA, PBGC should complete a Business Impact Analysis (BIA) in accordance with NIST guidance. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with the recommendation. WSD will work with ECD, ITIOD and all information system owners to ensure that the PBGC Corporate BIA, developed based upon Federal Continuity Directive 1 and 2, includes references to the critical systems and their respective BIA and Contingency Plan documentation. System-level BIA and Contingency plan documentation will be developed based upon NIST 800-34 and meet FISMA requirements
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-16: PBGC should use its BIA in determining the categorization and recovery time objective of the PLUS application. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with this recommendation. OBA will work with WSD to ensure the categorization and recovery time objective of the PLUS application is documented in the system-level BIA.
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-17: PBGC should ensure that security definitions across its systems and documentation are consistent. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with this recommendation. ECD will leverage its existing processes to ensure that the security definitions provided within NIST SP 800-34 are consistently applied in documentation across the enterprise.
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-18: PBGC should ensure that security documentation do not contradict each other and are consistent with its policy. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with this recommendation. ECD will work with stakeholders including WSD, OBA and ITIOD to ensure that security documentation regarding system-level BIAs and Contingency Plans are consistent and content does not conflict within documentation.
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-19: PBGC should develop and implement processes and procedures for effective communication of its security policies and processes. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with this recommendation. ECD will continue to improve its processes as an effort to better communicate all IT security policies and guidance through the agency's PPL library, ECD Bulletins, Data Calls, Cybersecurity and Privacy Council and Information System Security Officers (ISSO) Forum. ECD will continue to use these procedures to communicate any updates or new IT security policies and processes.
>
> **Scheduled Completion Date:** 6/30/2018

FISMA-16-20: PBGC should improve its process of communicating COOP test plans and test results to ensure errors in documentation is eliminated for effective reporting to its stakeholders. *(NFR 16-16)*

> **PBGC Response:** PBGC agrees with this recommendation. OIT will identify and implement necessary improvements to ensure COOP test plans are stored and maintained centrally and that COOP test results are documented correctly and communicated to the appropriate stakeholders in a timely and consistent manner.
>
> **Scheduled Completion Date:** 6/30/2017

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:
https://oig.pbgc.gov/hotline.html

Or Write:
Pension Benefit Guaranty Corporation
Office of Inspector General Hotline
1200 K Street NW, Suite 480
Washington, DC 20005