Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation Report

Fiscal Year 2015 Federal Information Security Modernization Act Final Report

February 19, 2016

FA-15-108-7/EVAL 2016-7

February 18, 2016

To: W. Thomas Reeder, Jr.
Director

From: Rashmi Bartlett
Assistant Inspector General for Audit

Subject: Fiscal Year (FY) 2015 Federal Information Security Modernization Act (FISMA) Report (FA-15-108-7/EVAL 2016-7)

I am pleased to transmit the final fiscal year (FY) 2015 Federal Information Security Modernization 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 the eight new recommendations in this report.

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

Attachment

cc:

Bob Scherer	Michael Rae	Tim Hurr
Judith Starr	Alice Maroni	Joshua Kossoy
Patricia Kelly	Ann Orr	Marty Boehm
Cathleen Kronopolus	Karen Morris	

CliftonLarsonAllen LLP
www.cliftonlarsonallen.com

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

Dear Mr. Westbrooks:

We are pleased to provide the Fiscal Year (FY) 2015 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 (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-16-03, *"Fiscal Year 2015-2016 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 the PBGC OIG. The OIG then reviewed, approved, and submitted the responses to OMB on November 13, 2015. 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 February 12, 2016) to the draft FISMA 2015 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
February 15, 2016

TABLE OF CONTENTS

Page

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization 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.

We are reporting fifteen FISMA findings with twenty-five (25) recommendations for FY 2015 based on the results of our FY 2015 independent evaluation. In addition to those in this report, there were nine (9) FISMA-related recommendations reported in the Corporation's FY 2015 internal control report based on our FY 2015 financial statements audit work. There is no overlap in the findings and recommendations in the two reports. PBGC took corrective actions on 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 thousand 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 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; for example, Congress must be notified of a "confirmed" breach within seven 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 2015 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, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST Special Publication 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 (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)
- Premium & Practitioner System (PPS)
- My Pension Benefit Administrator (MyPBA)

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, 2015 to September 30, 2015, at PBGC's headquarters in Washington, DC.

This independent evaluation was prepared based on information available as of September 30, 2015.

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.

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. Prior year information security material weaknesses have been downgraded to significant deficiencies in the FY 2015 financial statement internal control report, however, much work remains to continue progress in correcting these deficiencies. In this year's audit, we identified six new weaknesses; some recommendations remain from prior years and are noted below:

1. Entity-wide Security Program Planning and Management

PBGC has not fully implemented components of its entity-wide information security risk management program. However, PBGC made significant progress in addressing the Corporation's entity-wide security program planning and management control deficiencies. In FY 2015, new information technology (IT) security leadership provided the direction and guidance needed to implement a coherent framework of security controls to protect PBGC's information from unauthorized access, modification and disclosure. PBGC improved communication on the status and direction of IT security and introduced new policies, processes, procedures, and technology to effectively manage information security risks. We concurred in the closure of ten recommendations submitted for review. As a result, corrective actions taken by the Corporation have reduced the risk level of the entity-wide security program from a material weakness to a significant deficiency. These efforts, however, did not fully address the challenges faced by the Corporation to effectively implement an entity-wide information security program to manage its security process. OMB and the National Institute of Science and Technology (NIST) guidance requires agencies to have an effective entity-wide security program.[1] (See Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's FY 2015 and 2014 Financial Statements Audit (AUD-2016-3 /FA-15-108-3), issued November 13, 2015 - http://oig.pbgc.gov/pdfs/FA-15-108-3.pdf.)

2. Access Controls and Configuration Management

PBGC also made progress in addressing access controls and configuration management deficiencies noted in prior years. However, this progress did not fully resolve security weaknesses. Access controls and configuration management weaknesses remain a systemic

[1] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* and National Institute of Science and Technology (NIST) Special Publications (SP), including SP 800-53, Revision 4 *Security and Privacy Controls for Federal Information Systems and Organization*s, SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and SP 800-39, *Managing Information Security Risk.*

problem throughout PBGC. 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. PBGC has pushed out the dates for many planned corrective actions by one year or more. In FY 2015, PBGC's new IT security leadership implemented various tools and processes to establish a more coherent environment for implementing access control and configuration management security controls at the root cause level. We concurred with closing seven recommendations. As a result, corrective actions taken by the Corporation have reduced the risk level of access controls and configuration management from a material weakness to a significant deficiency. (See - http://oig.pbgc.gov/pdfs/FA-15-108-3.pdf for details.)

In addition, our audit also found deficiencies specifically related to responses required by OMB M-16-03, "*Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements"* (October 30, 2015) which are included in this report. These findings and recommendations, not previously reported, are as follows.

VI. FINDINGS AND RECOMMENDATIONS

1. Continuous Monitoring Management

a. Security Information and Event Management

PBGC has not fully implemented its operational intelligence solution for log management, data collection, storage and visualization (Splunk Enterprise). PBGC has not fully implemented Splunk Enterprise's security information and event management (SIEM) capability. Furthermore, current implementation only extends to the general support systems and does not include the major applications.

Splunk is not deployed to gather information on major applications. System owners of major applications have not determined the requirements for data collection, storage, indexing, searching, correlating, visualizing, analyzing and reporting on machine-generated data to identify and resolve operational and security issues.

PBGC's implementation of Splunk 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.

Per our review of the ITIOD-100-1398 *Security Incident Management Operational Procedures*, when a significant security event is generated, the security analyst should document attributes, determine if the activity is still occurring, and what was used to triage.

CLA inspected an example of analysts' comments for August 2015 and noted that analysis of those events was documented using the Event Analysis Checklist. However, PBGC did not provide a complete listing of events for August 2015 for CLA to confirm that all the events that were prioritized with an event urgency category of Critical or High were documented using the Event Analysis Checklist.

Recommendations:

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

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

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

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

b. Information Security Continuous Monitoring (ISCM) Program

PBGC has not fully established and implemented an entity-wide continuous monitoring 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.

Recommendations:

4. 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) (PBGC's Scheduled Completion Date: 6/30/2016)**

2. Configuration Management

a. Windows Native FTP

Window servers were operating with native FTP despite PBGC's plans to validate that native FTP had been removed from all servers by October 1, 2015. These servers did not meet PBGC's configuration baselines.

The use of native FTP is insecure as data would be transmitted as plaintext, which presents a risk of PBGC disclosing information to unauthorized persons.

Recommendations:

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

b. PBGC IP Address Inventory

In prior years, we noted PBGC did not use a centralized tracking repository to manage its inventory of Internet protocol (IP) addresses connected to the network, and identify assets for version control. Logging of patching and configuration changes was unreliable and vulnerability scans were incomplete. PBGC could not determine what assets were missing from its scans or what types of vulnerabilities were within its environment.

In FY 2015, PBGC implemented Infoblox to manage IP addresses. The technology has not fully matured, as standard operating procedures and guidance is being developed. The Corporation expects Infoblox training and full deployment will assist in resolving longstanding issues within inventory management.

Recommendations:

6. 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) (PBGC's Scheduled Completion Date: 6/30/2016)**

7. 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) (PBGC's Scheduled Completion Date: 6/30/2016)**

c. Credentialed Scanning

Credentialed scans grant local access to scan the target system. These authenticated network scans 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. A scanning agent often requires elevated privileges to access protected resources and read registries.

The FY 2015 CIO Annual FISMA Metrics Version 1.2, 30 July, 2015, asked agencies to provide percent (%) of hardware assets assessed using credentialed (privileged) scans with Security Content Automation Protocol (SCAP) validated vulnerability tools. PBGC has not fully implemented a credentialed scanning program. However, one of the groups responsible for scanning initiated a quarterly credentialed scanning program for some PBGC's systems in August 2015. This program did not provide coverage for all of PBGC. PBGC is in the process of developing and implementing a comprehensive credentialed scanning program for its systems.

Recommendation:

8. 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. 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.

- Technical controls have not been implemented to separate incompatible duties in PIMS.

Recommendations:

9. Develop and implement technical controls to separate incompatible duties in PIMS. **(OIG Control Number FISMA-13-15) (PBGC's Scheduled Completion Date: 12/31/2014*)**

b. Access Control

One of PBGCs main databases did not comply with PBGC's password and account lockout policy. Weaknesses in identification and authentication controls for one of PBGC's main databases increase the risk that individuals may obtain unauthorized access to PBGC systems, thus putting systems and data at risk of unauthorized disclosure, modification or destruction.

Recommendations:

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

10. PBGC ensures that password and account lockout settings for databases are updated to be consistent with PBGC requirements identified in the *PBGC Identification and Authentication*

Standard (SE-STD-01-27) and PBGC Access Control Standard (SE-STD- 01-32). **(OIG Control Number FISMA-15-06)**

4. Incident Response And Reporting

a. Incident Handling and Security Monitoring

PBGC purchased an automated tool to collect, analyze, search, and monitor information system security logs across the general support system. 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 has enhanced PBGC's detection of security events. However, PBGC has not implemented this tool for applications. When fully implemented across the PBGC, the tool will exponentially increase PBGC's detection of security events.

We identified the following weaknesses in PBGC's access controls over incidence response which created substantial risk of personally identifiable information (PII) or sensitive data exposure:

- Incident handling process was ineffective in monitoring, detecting, examining and reporting security incidents.
- 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.
- 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.

Recommendations:

11. 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) (PBGC revised date: 6/30/2016)**

12. Ensure that security incidents are documented, investigated, reported to federal management, and corrective actions implemented to remediate security vulnerabilities. **(OIG Control # FS-14-10) (PBGC revised date: 6/30/2016)**

13. Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk**. (OIG Control # FS-14-12) (PBGC revised date: 6/30/2017)**

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: 6/30/2016)**

5. Risk Management

a. 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 and 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.**

In FY 2014, per our review, three out of five employees sampled who had 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.

Workplace Solutions and Human Resources are working together to identify a plan to correct the discrepancy. Workplace Solutions and Human Resources are working to assess risk levels, review the position descriptions, and determine whether the current background investigation is acceptable. If the position's risk level increases then the employee's level of background investigation will also increase. Workplace Solutions will work with the employee to conduct a higher level background investigation.

Recommendations:

15. 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: 6/30/2016)**

b. Security Management

PBGC did not complete the annual security control assessment for one of its major applications in FY 2015. PBGC is not compliant with its policies for conducting the annual security control assessment. PBGC reported that continuous monitoring testing for the application was completed for Access Control, Awareness and Training, Audit and Accountability, and Security Assessment and Authorization. However, PBGC stated continuous monitoring testing was suspended due to resource constraints and the PBGC Security Team decided to rely on the A-123 review. The decision was not timely communicated to the Enterprise Cybersecurity Division (ECD) to request a waiver. A waiver for the MyPAA continuous monitoring testing was requested and signed by ECD on December 10, 2015. The major application security assessment and authorization is expected to start in early FY 2016.

Weaknesses in security controls assessment increases the risk that security controls in the major application are not operating as intended. Additionally, there is the risk that system resources may not be fully protected if security controls are not assessed on a continuous basis and also in compliance with FISMA requirements. PBGC could be exposed to increased risk of data modification or deletion. Also, there is the risk of not identifying residual vulnerabilities within the application and providing credible and meaningful inputs to the PBGC's Plan of Action and Milestones (POA&M), and supporting the major application's Authorizing Official's accreditation decision.

Recommendation:

16. 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)**

6. Security Training

a. Security Awareness Training

PBGC did not ensure that all personnel with significant IT security responsibilities completed the required role-based training in FY 2015. Specifically, we noted that:

- Thirteen (13) out of forty nine (49) PBGC personnel with significant IT security responsibilities (security training for Authorizing Officials, Information System Owners, Information System Security Officers, Common Control Providers and Incident Response Handlers) who were required to take role-based training for FY 2015 did not complete the training.

Weaknesses in security role-based training controls increase the risk that users may not be aware of their responsibilities for protecting PBGC systems and data. This could result in unauthorized access to PBGC systems and data.

Recommendation:

17. PBGC should increase records management controls and monitoring to ensure all required personnel timely complete role-based training. **(OIG Control Number FISMA-15-08)**

7. Contractor Systems

a. Review of Interconnection Security Agreements

In FY 2013 and FY 2014, PBGC's process for documenting its interconnection security agreements with other entities had outdated documents and incomplete attachments; the tracking document was also incomplete. In FY 2015, ECD completed a gap analysis of interconnection security agreements against the OMB Circular A-130 Appendix III, NIST SP 800-47, and NIST SP 800-53 requirements.

Recommendations:

18. Ensure the Information Security Agreement Tracking Document is reviewed for accuracy and completeness. **(OIG Control Number FISMA-13-17) (PBGC's Scheduled Completion Date: 6/30/2016)**

19. Review the Information Security Agreements to ensure they are current and complete. **(OIG Control Number FISMA-13-18) (PBGC's Scheduled Completion Date: 6/30/2016)**

8. Privacy

a. 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. In FY 2015, PBGC completed the installation of the data masking solution. However, PBGC is still in the process of developing and testing masking templates.

Recommendations:

20. Remove PII from the development environment**. (OIG Control Number FISMA-11-02) (PBGC's Scheduled Completion Date: 6/30/2016)**

b. Information Technology Controls for the Protection of Privacy - PBGC Connect

PBGC's Site Collection Owners did not establish or document a policy governing the use of PBGC Connect sites (i.e. SharePoint). In FY 2015, about 15-20% of business units were using SharePoint. The Site Collection Owners were accountable for all of the sites, content, and administrative settings within their assigned site collection(s). The Site Collection Owners had not developed policy for site users.

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. This is a manual intensive process that does not catch all instances of PII in SharePoint.

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 is not protected from disclosure and is not reported as PBGC is unaware of the violation.

Recommendations:

21. 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 determine and implement any additional, business-specific guidance required for their sites. **(OIG Control Number FISMA-14-01) (PBGC's Scheduled Completion Date: 3/31/2016)**

22. 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's Scheduled Completion Date: 3/31/2016)**

23. 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's Scheduled Completion Date: 3/31/2016)**

24. 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) (PBGC's Scheduled Completion Date: 6/30/2015*)**

25. 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) (PBGC's Scheduled Completion Date: 6/30/2016)**

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 2015 and 2014 Financial Statements Audit* (*AUD 2016-3/FA-15-108-3*) issued November 13, 2015.

Finding Summary	Recommendation
1. Entity-wide Security Program Planning and Management PBGC made significant progress in addressing the Corporation's entity-wide security program planning and management control deficiencies. In FY 2015, new information technology (IT) security leadership provided the direction and guidance needed to implement a coherent framework of security controls to protect PBGC's information from unauthorized access, modification and disclosure. PBGC improved communication on the status and direction of IT security and introduced new policies, processes, procedures, and technology to effectively manage information security risks. We concurred in the closure of ten recommendations submitted for review. As a result, corrective actions taken by the Corporation have reduced the risk level of the entity-wide security program from a material weakness to a significant deficiency. These efforts, however, did not fully address the challenges faced by the Corporation to effectively implement an entity-wide information security program to manage its security process. OMB and the National Institute of Science and Technology (NIST) guidance requires agencies to have an effective entity-wide security program.[2] 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	***Recommendations:*** • 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)** • 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)** • 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)**

[2] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources,* and National Institute of Science and Technology (NIST) Special Publications (SP), including SP 800-53, Revision 4 *Security and Privacy Controls for Federal Information Systems and Organization*s, SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and SP 800-39, *Managing Information Security Risk.*

Finding Summary	Recommendation
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 critical resources. PBGC has not fully implemented components of its entity-wide information security risk management program. Some components not fully implemented include the following: • Implementing common controls and remediating common control weaknesses. • Making all common controls compliant with NIST SP, Revision 4, *Security and Privacy* • *Controls for Federal Information Systems and Organizations* requirements. • Making all common controls available to system owners for appropriate inclusion in their system security plans. • Completing the transition to the PBGC Risk Management Framework (RMF) supports PBGC organizational, mission and information system objectives by addressing each of the six RMF phases: categorize, select, implement, assess, authorize, and monitor. • Fully implementing a continuous monitoring program. • Completing the transition to NIST 800-53, Revision 4 security controls. PBGC is cognizant of these challenges and in July 2015, implemented NIST's RMF to establish an integrated enterprise-wide decision structure for cybersecurity risk management that includes and integrates PBGC mission and business areas. Implementation of the Framework supports PBGC organizational, 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 has established a timeline for transition to the RMF requirements by September 2016.	

Finding Summary	Recommendation
2. Access Controls and Configuration Management PBGC also made progress in addressing access controls and configuration management deficiencies noted in prior years. In FY 2015, PBGC's new IT security leadership implemented various tools and processes to establish a more coherent environment for implementing access control and configuration management security controls at the root cause level. We concurred with closing seven recommendations. As a result, corrective actions taken by the Corporation have reduced the risk level of access controls and configuration management from a material weakness to a significant deficiency. However, this progress did not fully resolve security weaknesses. Access controls and configuration management weaknesses remain a systemic problem throughout PBGC. 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. PBGC has 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 weaknesses in PBGC's information system security controls. PBGC has not fully addressed access controls and configuration management weaknesses. Some controls not fully implemented include the following: • Developing and implementing a coherent strategy and approach for providing information services and information system management controls, correcting IT infrastructure deficiencies, developing a framework for implementing common security controls, mitigating the systemic issues related to access control, and strengthening system configurations and user account management for all of PBGC's information systems. • Developing and implementing an account	***Recommendations:*** • Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems. **(OIG Control # FS-09-12) (PBGC revised completion date: June 30, 2016*)** • 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 completion date: June 30, 2016*)** • 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 completion date: June 30, 2016*)** • Appropriately restrict developers' access to production environment to only temporary emergency access. **(OIG Control # FS-07-10) (PBGC revised completion date: June 30, 2016*)** • 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 # FS-07-12) (PBGC revised completion date: June 30, 2016*)** • Continue to remove unnecessary user and generic accounts. **(OIG Control # FS-07-08) (PBGC revised completion date: June 30, 2016*)**

Finding Summary	Recommendation
management monitoring program that ensures that accounts are constantly maintained in accordance with PBGC account management standards and that reduces the dependency on recertification. • Implementing infrastructure controls and access controls to restrict developers' access to the production environment. • Developing the process and procedures for utilizing the security configuration checklists in the establishment of baseline configurations for each information system technology product. • Developing and implementing 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 PBGC systems. • Developing and implementing a checklist to assist contracting officers in their efforts to acquire IT assets and services that comply with both PBGC and federal policy requirements. 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 components2 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 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 2015

OIG Control Number	Date Closed	Original Report Number
FISMA-09-08		AUD-2010-6/FA-09-64-6
FISMA-09-09		AUD-2010-6/FA-09-64-6
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-13-16		EVAL-2014-9/FA-13-93-7
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-14-13		EVAL 2015-9/FA-14-101-7
FISMA-14-14		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-14-21		EVAL 2015-9/FA-14-101-7

IX. PRIOR AND CURRENT YEARS' OPEN FISMA RECOMMENDATIONS

OIG Control Number	Original Report Number
Prior Year	
FISMA-11-02	EVAL-2012-9/FA-11-82-7
FISMA-13-15	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
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-14-11	EVAL 2015-9/FA-14-101-7
FISMA-14-12	EVAL 2015-9/FA-14-101-7
FISMA-14-15	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
FS-14-09	AUD-2015-3/FA-14-101-3
FS-14-10	AUD-2015-3/FA-14-101-3
FS-14-11	AUD-2015-3/FA-14-101-3
FS-14-12	AUD-2015-3/FA-14-101-3
FS-07-17	AUD-2009-3/FA-07-XX-XX

OIG Control Number	**Original Report Number**
Current Year	
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-15-06	(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)

X. MANAGEMENT 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 12 2016

To: Robert A. Westbrooks
Inspector General

From: W. Thomas Reeder

Subject: Response to OIG's Draft Fiscal Year 2015 FISMA Report

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, dated January 29, 2016, relating to FY 2015 compliance with the Federal Information Security Management Act (FISMA). Your office's work on this is sincerely appreciated.

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 CPO
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:

1. Continuous Monitoring Management

Security Information and Event Management

FISMA-15-01: *Fully implement Splunk Enterprise in PBGC, including its SIEM capability. (NFR 15-11)*

PBGC Response: PBGC agrees with the recommendation. OIT recognizes that Splunk is a multi-faceted tool and believes it is important to define "fully implement". OIT has created a POA&M to define what "fully implement Splunk Enterprise" means, taking into consideration the needs of the agency and the IG's recommendation. Once that definition is socialized with the appropriate leadership, a new POA&M or POA&Ms will be developed to complete the defined implementation of Splunk.

Scheduled Completion Date: 6/30/2017

FISMA-15-02: *Require system owners to fully implement Splunk Enterprise for PBGC major applications. (NFR 15-11)*

PBGC Response: PBGC agrees with the recommendation. As with the first recommendation, OIT will create a definition of "fully implement", as that relates to use of Splunk by the business areas. Once that definition is socialized with the appropriate leadership, a new POA&M or POA&Ms will be developed to complete the defined implementation of Splunk by the business areas. In the meantime, it should be noted that efforts are currently underway to define auditable events for each major application and to incorporate those definitions into the overall use of Splunk. Those efforts will continue until further refined, as described above.

Scheduled Completion Date: 6/30/2017

FISMA-15-03: *Ensure the consistent use of the Event Analysis Checklist as part of the event analysis process. (NFR 15-11)*

PBGC Response: PBGC agrees with the recommendation. OIT will review the Monthly Review and Oversight process and the Event Analysis Checklist to ensure they are in alignment. OIT will also review the oversight process to ensure that exceptions like those noted in the finding are detected and resolved. OIT is in the process of creating a POA&M to ensure this weakness is appropriately remediated.

Scheduled Completion Date: 6/30/2016

2. Configuration Management

Windows Native FTP

FISMA-15-04: *PBGC should remove native FTP from any remaining systems. (NFR 15-16)*

PBGC Response: PBGC largely agrees with this recommendation. Although we are working to eliminate native FTP where possible, we have noted exceptions that were approved via the risk acceptance process and configured within the IEM as non-compliant exceptions. As noted in the NFR, POA&M 1253 will address the control deficiency that allowed the noted condition, the six non-risk accepted systems running native FTP, to occur. The condition identified in this NFR has been remediated via RFC C002379 - Disable FTP Services on the PBGC Web Servers (Production Only).

Scheduled Completion Date: 6/30/2016

Credentialed Scanning

FISMA-15-05: *Perform scheduled credentialed scans to include all the systems and update PBGC policies and procedures to require regular credentialed scans. (NFR 15-13)*

PBGC Response: PBGC agrees with the recommendation. It should be noted that properly incorporating credentialed scanning will require PBGC to devote significant additional resources that must be planned for, requested and approved. ECD has begun to pilot credentialed scanning of business applications, from the compliance and oversight perspectives. ITIOD is currently exploring what is required to implement credentialed scanning of the GSS, as well as the resources and process changes needed to ingest and respond appropriately to the vulnerabilities discovered through all types of credentialed scanning. Multiple POA&Ms are either in progress or will be developed to address the credentialed scanning issues identified.

Scheduled Completion Date: 6/30/2017

3. Identity and Access Management

Access Control

FISMA-15-06: *PBGC ensures that password and account lockout settings for databases are updated to be consistent with PBGC requirements identified in the PBGC Identification and Authentication Standard (SE-STD-01-27) and PBGC Access Control Standard (SE-STD-01-32). (NFR 15-16)*

PBGC Response: PBGC agrees with this recommendation. OIT has created POA&Ms 1231 and 1217 to remediate weaknesses in password management and account management automation respectively, and will consider computing differences between Windows and Unix-based system components in these remediation efforts. OIT has also created POA&M 1253 to ensure consistent implementation of standard settings that comply with SE-STD-01-27 (last updated 06/30/2015 and submitted as evidence for the

FY15 audit…the excerpt from the standard above is not from this latest version) and SE-STD-01-32 (last updated 08/01/2013) across the enterprise.

Scheduled Completion Date: 6/30/2017

4. Risk Management

Security Management

FISMA-15-07: *Evaluate existing controls and determine effectiveness to ensure annual security control assessments are timely completed for all major applications and general support systems.*

PBGC Response: PBGC agrees with the recommendation. OIT will work with business areas to ensure all planned system-level continuous monitoring activities are completed as defined in PBGC's Risk Management Framework (RMF) process. OIT has created POA&M 2066 to address this recommendation.

Scheduled Completion Date: 6/30/2017

5. Security Training

Security Awareness Training

FISMA-15-08: *PBGC should increase records management controls and monitoring to ensure all required personnel timely complete role-based training. (NFR 15-15)*

PBGC Response: PBGC agrees with the recommendation. OIT recognizes that Role-Based Training (RBT) needs to be improved, and designation letters will be reviewed and reissued to require training. OIT has created POA&M 2043 to address this recommendation.

Scheduled Completion Date: 12/31/2016

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