



OFFICE OF INSPECTOR GENERAL EVALUATION REPORT

Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report

**Report No. EVAL-2018-7
December 20, 2017**



Office of Inspector General
Pension Benefit Guaranty Corporation

December 20, 2017

TO: Thomas Reeder
Director

FROM: Nina Murphy *NM*
Assistant Inspector General for Audits, Evaluations, and Reviews

SUBJECT: Issuance of Fiscal Year 2017 Federal Information Security Modernization Act
Independent Evaluation Report (EVAL-2018-7/FA-17-119-6)

I am pleased to transmit the fiscal year 2017 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 agreed with the five new recommendations in this report.

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

cc: Patricia Kelly, Chief Financial Officer
Cathy Kronopolus, Chief of Benefits Administration
Alice Maroni, Chief Management Officer
Karen Morris, 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



CliftonLarsonAllen

**Fiscal Year 2017 Federal Information Security Modernization Act
Independent Evaluation of the Pension Benefit Guaranty Corporation**

December 15, 2017

December 15, 2017

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) 2017 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 and practices.

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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-18-02, *Fiscal Year 2017-2018 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 October 31, 2017. This evaluation report provides additional information on the results of our review of PBGC's information security program and information systems.

In preparing the 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 December 12, 2017) to the draft FISMA 2017 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.



Greenbelt, Maryland

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Table of Contents

Executive Summary	1
Background	2
Summary of Results	5
Security Function: Identify	8
<i>Metric Domain – Risk Management.....</i>	<i>8</i>
Security Function: Protect	11
<i>Metric Domain – Configuration Management.....</i>	<i>11</i>
<i>Metric Domain – Identity and Access Management.....</i>	<i>11</i>
<i>Metric Domain – Security and Privacy Training.....</i>	<i>12</i>
Security Function: Detect.....	14
<i>Metric Domain – Information Security Continuous Monitoring (ISCM)</i>	<i>14</i>
Security Function: Respond	16
<i>Metric Domain – Incident Response</i>	<i>16</i>
Security Function: Recover.....	17
<i>Metric Domain – Contingency Planning</i>	<i>17</i>
Appendix A: Scope and Methodology.....	19
Appendix B: Status of Prior-Year Recommendations	21
Appendix C: Management Comments	23

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

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.

The Pension Benefit Guaranty Corporation (PBGC or the Corporation) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP to perform the fiscal year (FY) 2017 FISMA evaluation. The objective of this evaluation was to determine the extent to which the PBGC's information security program and practices complied with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable OMB and National Institute for Standards and Technology (NIST) guidance.

The FISMA evaluation requires us to assess the maturity of five functional areas in PBGC's information security program.¹ This assessment used objective metrics that are standardized across the Federal government. To be considered effective, an agency's IT security must be rated *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5). PBGC did not reach that level. Four of the five functional areas at PBGC achieved a maturity level of *Consistently Implemented* (Level 3). One function, *Protect*, was found to be *Defined* (Level 2).

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 conclude that PBGC's information security program still needs improvement. Specifically, we noted weaknesses in risk management, vulnerability and configuration management, identity and access management, information security continuous monitoring, and contingency planning.

To address these weaknesses, we are reporting 24 recommendations of which five are new for this year based on the results of our FY 2017 independent evaluation. In addition to those in this report, there were eleven FISMA-related recommendations reported in the Corporation's FY 2017 internal control report based on our FY 2017 financial statements audit work. There is no overlap in the findings and recommendations in the two reports.

¹ The FY 2017 metrics are based on a maturity model approach begun in prior years and align the metrics with all five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover.

Background

Corporation Overview

The PBGC protects the pensions of more than 40 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 information technology. 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.

FISMA Legislation

The Federal Information Security Modernization Act of 2014² (FISMA) provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency's Chief Information Officer (CIO) or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

² The Federal Information Security Modernization Act of 2014 (Public Law 113-283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

FISMA also requires agency IGs to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

FY 2017 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. During FY 2017, OMB and DHS leveraged the Chief Information Officer and Inspector General FISMA metrics to assess federal civilian agencies' risk management to comply with Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

The FY 2017 metrics are based on a maturity model approach begun in prior years and align the metrics with all five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity agency-wide risks across the enterprise IT and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 1**.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2017 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model spectrum focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 2** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*. This is the first year in which the complete maturity model, with its objective scoring, has been available.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Table 2: IG Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Summary of Results

PBGC continues to make progress in improving its information security and privacy program and its compliance with FISMA, OMB requirements, and applicable NIST guidance. Specifically, it closed 11 out of 30 open recommendations from prior year FISMA evaluations. In FY 2017, PBGC focused on resolving its long-standing Entity-wide Security Management weaknesses and continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. PBGC realizes it requires cycle time and institutional maturity to fully resolve these security weaknesses. However, continued focus is needed to effectively remediate the remaining risks and weaknesses associated with risk management, access and configuration management controls.

Current Results

Despite the noted progress, PBGC must make additional improvements to achieve effective information security. Weaknesses identified in this evaluation include weaknesses in the areas of risk management, vulnerability and configuration management, identity and access management, information security continuous monitoring, and contingency planning.

Our conclusions as to the effectiveness of PBGC's IT security incorporate multiple sets of results, are set forth below.

1. FISMA maturity scores

FISMA requires evaluators across the Federal government to respond to 61 objective questions, from which a DHS algorithm calculates a maturity score for each of five functional areas. As set forth in the chart below, PBGC was rated at *Consistently Implemented* (Level 3) in four of the five functional areas. One functional area, *Protect*, was found to be at the *Defined* (Level 2).³ Thus, by these objective metrics, PBGC fell below the specified threshold of effectiveness, which is level 4, *Managed and Measurable*.

Table 3 below summarizes the maturity ratings and assessment by function.

³ The most frequent maturity level rating across the Protect function served as the overall Protect function rating.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Table 3: FY 2017 IG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions⁴	Metric Domains	Calculated Maturity Level	Cyberscope Evaluation
Identify	Risk Management	Consistently Implemented (Level 3)	Not Effective
Protect	Configuration Management	Consistently Implemented (Level 3)	Not Effective
	Identity and Access Management	Defined (Level 2)	Not Effective
	Security Training	Defined (Level 2)	Not Effective
Detect	Information Security Continuous Monitoring	Consistently Implemented (Level 3)	Not Effective
Respond	Incident Response	Consistently Implemented (Level 3)	Not Effective
Recover	Contingency Planning	Consistently Implemented (Level 3)	Not Effective
Overall	Not Effective		

2. Detailed Findings

While PBGC has made progress in addressing the security weaknesses noted in prior years, work still remains to continue correcting these deficiencies. In this year's audit, we identified areas in the information security program that require strengthening. **Table 4** below summarizes our detailed findings.

Table 4: Findings Noted During the FY 2017 FISMA Evaluation of PBGC

IG FISMA Metric Domain	Findings
Risk Management	Ongoing authorization documentation was not maintained in the official and authoritative repository for system authorization and risk management.
	Risk management process documentation was not updated to clearly establish requirements.
	Lack of an insider threat detection and prevention program.

⁴ See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

IG FISMA Metric Domain	Findings
	Incomplete implementation of common security controls.
	Incomplete control implementation and assessment, and inadequate documentation of control inheritance for the general support system.
Configuration Management	Ineffective patch and vulnerability management process for remediation of vulnerabilities.
	Noncompliance with web server baseline configuration.
	Inadequate data loss prevention controls.
Identity and Access Management	Incomplete improvements for removal of separated and inactive accounts from applications.
	Incomplete remediation of background reinvestigation weaknesses.
	Identified authentication weaknesses from vulnerability assessment and penetration test.
Information Security Continuous Monitoring	Incomplete implementation of security information and event management tool (SIEM).
	Inadequate credential vulnerability scanning program.
	Inadequate data loss prevention controls.
	Network monitoring weaknesses.
Contingency Planning	Inadequate business impact analysis for the enterprise and applications.
	Incomplete update of security definitions for contingency planning.
	Incomplete update of system impact ratings to eliminate contradictions.

Overall, we conclude that information security at PBGC has improved in a number of areas. With continued effort, attention and investment, the information security program will mature and can cross the effectiveness threshold in the near future. At the present, however, the weaknesses that we identified leave PBGC operations and assets at risk of unauthorized access, misuse and disruption. To address these weaknesses, we are reporting 24 recommendations of which five are new for this year. One of five new recommendations for FY 2017 was a recommendation that had downgraded from the Financial Statement Internal Control Report to the FISMA report. The recommendation was previously associated with the Entity-wide Security Management significant deficiency that was primarily remediated by PBGC.

The following section provides the detailed findings by the security functions of Identify, Protect, Detect, Respond, and Recover.

Security Function: Identify

Overview

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 should 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. PBGC's risk management process still requires time to mature to be an effective continuous monitoring tool.

Metric Domain – Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, is guidance for implementing the risk management framework controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

We identified the following information security weaknesses in the Risk Management domain:

- PBGC's official and authoritative repository for system authorization and risk management did not properly maintain current documentation as part of its continuous monitoring program and was, in some cases, out of date. Specifically, PBGC did not consistently review, approve, update and upload required system security documentation in Cyber Security Assessment and Management (CSAM) for several of its systems.

In FY 2016, PBGC had systems in ongoing authorization without the correct, finalized, and up-to-date system security documentation recorded in the CSAM tool 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. The required security documentation is maintained in CSAM as artifacts to support the system was authorized in accordance with the RMF.

In addition, the *PBGC Information Security Risk Management Framework Process* was not clear on the requirements for maintaining the Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), and Authorization to Operate (ATO) package in the "Status and Archive" container in CSAM.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

In FY 2017, we noted that the Enterprise Cybersecurity Division (ECD) began quarterly reviews of the “Status and Archive” page in CSAM to identify missing artifacts. Also, ECD has provided updates to clarify these requirements for maintaining the POA&M and SAR generated for the ATO package. Further, ECD has updated the PBGC RMF process to more clearly state where system security documentation and artifacts are required to be loaded into CSAM. However, the updated RMF process was not completed until the end of FY 2017 and therefore, we were not able to assess the implementation of the updated policy.

- Changes in threats and security requirements were not assessed, and strategies for mitigating additional risks were not updated and/or developed for the General Support System (GSS) risk assessment in the prior year. In addition, the PBGC RMF process did not include a requirement to annually review or conduct a risk assessment. In FY 2017, ECD reviewed the PBGC RMF process to clarify the requirement for reviewing the Risk Assessments annually. ECD plans to conduct a briefing to discuss the updates to the RMF process. Therefore, the process has not been fully implemented.
- PBGC did not implement an insider threat detection and prevention program in FY 2017. 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. PBGC has not created a cross-discipline insider threat incident handling team. However, PBGC did delegate a senior PBGC official on July 25, 2017, to be the responsible individual to implement and provide oversight for the insider threat program.
- PBGC did not complete the implementation of NIST SP 800-53, Revision 4, controls that were designated as common controls,⁵ remediate common controls weaknesses and did not make the common controls available to system owners in CSAM for appropriate inclusion in their system security plans.
- The general support system owner did not complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4, did not revise its inheritance of common controls, nor conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4.

Without effective risk management controls, PBGC is at risk of controls not operating as intended, increasing the likelihood of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information.

Recommendations:

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

- Revise the processes and procedures of the continuous monitoring program to consistently enforce the review, update, and uploading of all required security assessment and authorization documentation for each system before the documentation expires.
(FISMA-17-01)

⁵ A common control is a security control that is inheritable by one or more organizational information systems.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

- 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) (PBGC completion date: June 30, 2018)**
- 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) (PBGC completion date: June 30, 2018)**
- 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) (PBGC completion date: June 30, 2018)**
- 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) (PBGC completion date: December 31, 2017)**
- PBGC should assign a senior organizational official, and develop and implement an insider threat detection and prevention program. **(OIG Control Number FISMA-16-14) (PBGC completion date: June 30, 2018)**
- 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: June, 30, 2018)**
- Complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4, revise the inheritance of common controls, and conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4. **(OIG Control Number FISMA-17-02)**

Security Function: Protect

Overview

In FY 2017, PBGC continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. However, PBGC has realized it requires cycle time and institutional maturity to fully resolve some security weaknesses. Weaknesses in the PBGC IT environment continue to contribute to deficiencies in system configuration, and access controls.

Metric Domain – Configuration Management

To secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. OMB requires all workstations that use Windows to conform to the U.S. Government Configuration Baseline standards. Furthermore, NIST has developed a repository of secure baselines for a wide variety of operating systems and devices.

We noted the following information security weaknesses in the Configuration Management domain:

- PBGC had an ineffective patch and vulnerability management process to remediate vulnerabilities identified in vulnerability assessment scans.
- PBGC web servers were not in compliance with baseline configurations.

The details related to PBGC's vulnerability management program, data loss prevention, patch management, and configuration management weaknesses were noted in the FY 2017 Vulnerability Assessment and Penetration Test Report, dated October 31, 2017. The following technical recommendations were issued in the restricted report: OIT-158R, OIT-160R, OIT-161R, OIT-164R, OIT-165R and OIT-166R.

Control weaknesses in the Configuration Management domain exposes PBGC to increased risk of compromise. Thus, PBGC may not have reasonable assurance regarding the confidentiality, integrity and availability of information in its systems.

Metric Domain – Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized to access information and information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a user name and password serve as the primary means of authentication, and the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. Homeland Security Presidential Directive 12 calls for all Federal departments to require personnel to use personal identity verification (PIV) cards. This use of PIV cards is a major component of a secure, government-wide account and identify management system.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

We noted the following information security weaknesses in the Identity and Access Management domain:

- PBGC did not complete the enhancements needed in its process for removing separated and inactive accounts from its applications and the GSS. We continued to find separated and inactive accounts during our review of access controls in FY 2017. The IT Infrastructure Operations Department (ITIOD) worked in conjunction with the Workplace Solutions Department (WSD) and the Quality Management Department to develop an updated separation process that would streamline tracking of separation actions, reduce manual steps, make reporting easier, and support compliance with our documented separation procedure. Updates to the separation-related coding in the service desk applications (GetIT and Service Manager 9) went into production on June 23, 2017. However, the updated separation process was recently implemented and therefore, there has not been enough cycle time to assess the effectiveness of the new process.
- Weaknesses in the background reinvestigation process continued to exist. Specifically, Title 5 Code of Federal Regulations Part 1400, *Designation of National Security Positions*, required agencies to re-designate each federal position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. In FY 2017, PBGC's WSD led the Position Re-designation Initiative in partnership with the Human Resources Department. WSD Security is in the process of initiating reinvestigations for the applicable individuals. However, WSD Security is not scheduled to complete the re-designation of PBGC Federal positions until December 31, 2017.

The details related to PBGC's vulnerability management program and authentication weaknesses were noted in the FY 2017 Vulnerability Assessment and Penetration Test Report, dated October 31, 2017. The following technical recommendations were issued in the restricted report: OIT-162R and OIT-163R.

Control weaknesses in the Identity and Access Management domain exposes PBGC to increased risk of compromise. Thus, PBGC may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Metric Domain – Security and Privacy Training

FISMA requires all Federal Government personnel and contractors to complete annual security and privacy awareness training that provides instructions on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot ensure that personnel would have the knowledge required to ensure the security of the information systems and data.

We did not find weaknesses in PBGC's Security and Privacy Training domain.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Recommendations:

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

- Document and implement enhanced process and procedures to effectively track and remediate known vulnerabilities in a timely manner. **(OIG Control Number: FISMA-17-03)**
- PBGC should implement effective process and procedures to ensure the secure configuration of web servers in accordance with the established configuration baselines and document deviations to the established baselines on an as needed basis. **(OIG Control Number: FISMA-17-04)**
- 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, 2018)**
- 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) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should provide training to Federal Managers and Contracting Officer's Representatives 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) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should enhance the process for removing separated and inactive accounts to include applications, not just Active Directory. **(OIG Control Number FISMA-16-12) (PBGC's Scheduled Completion Date: June 30, 2018)**

Security Function: Detect

Overview

In FY 2017, PBGC continued to enhance implementation of various tools and processes to detect threats and vulnerabilities to improve its continuous monitoring program. With the continued maturity and deeper implementation of these tools and processes, PBGC's continuous monitoring program will become more effective.

Metric Domain – Information Security Continuous Monitoring (ISCM)

The goal of ISCM is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to Federal systems and information. ISCM provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

We noted the following information security weaknesses in the Information Security Continuous Monitoring domain:

- PBGC did not complete its implementation of the security information and event management (SIEM) tool to fully maximize its capabilities. For example, the extension of the SIEM capability to include coverage for PBGC's major applications had not been completed.
- PBGC did not improve its credential⁶ vulnerability scanning program to reduce the number of credential failures.
- PBGC did not implement adequate data loss prevention controls to address weaknesses in its perimeter defenses.

The details related to PBGC's vulnerability management program and network monitoring weaknesses were noted in the FY 2017 Vulnerability Assessment and Penetration Test Report, dated October 31, 2017. The following technical recommendations were issued in the restricted report: OIT-155R and OIT-157R.

Control weaknesses in the Information Security Continuous Monitoring domain continue to expose PBGC to threats and vulnerabilities that could bypass its defenses, which may result in compromise and increased risk of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information. Thus, PBGC may not have reasonable assurance regarding the confidentiality, integrity and availability of information in its systems.

⁶ The credentialed scan utilized a user ID and password to enumerate the locally installed software and identified vulnerabilities from the user perspective. The credentialed scan summarized risks and vulnerabilities associated with remote attacks that leverage actions by the user as in phishing attacks and browsing malicious web content.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

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) (PBGC's Scheduled Completion Date: June 30, 2018)**
- Require system owners to fully implement Splunk Enterprise for PBGC major applications. **(OIG Control Number FISMA-15-02) (PBGC's Scheduled Completion Date: June 30, 2018)**
- 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) (PBGC's Scheduled Completion Date: to be determined)**
- 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's Scheduled Completion Date: June 30, 2018)**
- 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's Scheduled Completion Date: to be determined)**

Security Function: Respond

Overview

In FY 2017, PBGC met its established timelines for responding to security incidents and followed its processes and procedures for handling incidents.

Metric Domain – Incident Response

Information security incidents occur on a daily basis. Agencies must have sound policies and planning in place to respond to these incidents and report them to the appropriate authorities. The United States Computer Emergency Readiness Team is to receive reports of incidents on unclassified Federal Government systems, and OMB requires the reporting of incidents that involve sensitive data, such as personally identifiable information, within strict timelines.

We did not find weaknesses in PBGC's Incident Response program.

Recommendations:

None

Security Function: Recover

Overview

PBGC has a well established process and program for testing its contingency plan, but gaps remain in improving its effectiveness. PBGC has an annual program to test its contingency plan and update the planning documents based on lessons learned from the test exercise.

Metric Domain – Contingency Planning

FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if loss of a system's availability occurs. Consideration of risk to an agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. 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." Once a contingency plan is established, training and testing must be conducted to ensure that the plan and individuals tasked with the contingency responsibilities will be capable in the event of an emergency.

We noted the following information security weaknesses in the Contingency Planning domain:

- PBGC's 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 was in the process of updating its BIA with plans to issue the new PBGC-wide BIA in the Fall of 2017.
- During FY 2016, the PLUS application BIA did not meet NIST SP 800-34, Revision 1 requirements for a BIA. In FY 2017, the Office of Benefits Administration (OBA) conducted a PLUS BIA based on NIST SP 800-34 and incorporated the results into the PLUS Contingency Plan. However, OBA may update the PLUS Contingency Plan once the new PBGC-wide BIA is issued to ensure consistency with the Corporation wide contingency plans.
- During FY 2016, PBGC indicated that definitions and rating of the PLUS application's availability in CSAM were system specific and not uniform for all systems. In FY 2017, ECD leveraged its existing processes to confirm security definitions provided within NIST SP 800-34 are consistently applied in documentation across the enterprise. ECD plans to conduct a quality assurance check of its security definitions in FY 2018.
- In FY 2016, we noted there were inconsistencies between security documentation for PLUS and the availability impact rating was incorrectly identified as "Low" instead of "Moderate." Inconsistencies were found between PBGC's FIPS 199 Categorization of

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

PLUS, CSAM, PLUS' High Value Asset designation, PBGC's Annual COOP Exercise Test Plan, and PLUS System Security Plan.

In FY 2017, ECD worked with stakeholders including WSD, OBA and ITIOD to confirm security documentation regarding system-level BIAs and Contingency Plans were consistent and no conflicts existed. In FY 2018, ECD will review the effectiveness of its communications methodologies to determine the best methods to engage stakeholders. Any changes resulting from the review would be made to the ECD Communications Plans, where needed. In addition, stakeholders would also be notified of changes. The plan review will be included in the FY 2018 Policy Roadmap.

Control weaknesses in the contingency planning domain could result in improper development and implementation of appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to an incident or event.

Recommendations:

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

- As required by FISMA, PBGC should complete a Business Impact Analysis (BIA) in accordance with NIST guidance. **(OIG Control Number FISMA-16-15) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should use its BIA in determining the categorization and recovery time objective of the PLUS application. **(OIG Control Number FISMA-16-16) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should ensure that security definitions across its systems and documentation are consistent. **(OIG Control Number FISMA-16-17) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should ensure that security documentation do not contradict each other and are consistent with its policy. **(OIG Control Number FISMA-16-18) (PBGC's Scheduled Completion Date: June 30, 2018)**
- PBGC should develop and implement processes and procedures for effective communication of its security policies and processes. **(OIG Control Number FISMA-16-19) (PBGC's Scheduled Completion Date: June 30, 2018)**

Appendix A: Scope and Methodology

Scope

Our audit was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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.

The objective of this evaluation was to determine the extent to which PBGC's information security program and practices complied with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance.

The evaluation team performed a vulnerability and penetration test, and evaluated management, operational, and technical controls supporting major applications and general support system in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. The information security policies, procedures, and practices of the following PBGC systems were evaluated during FY 2017:

- Consolidated Financial System (CFS)
- Trust Accounting System (TAS)
- Premium and Practitioner System (PPS)
- Pension Lump Sum (PLUS) Program
- Information Technology Infrastructure Services General Support System (ITISGSS)
- Office 365 Multi-Tenant (O365 MT)

In addition, our evaluation included an assessment of effectiveness for each of the seven FY 2017 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions.

We performed our review from April 4, 2017 to September 30, 2017, at PBGC's headquarters in Washington, DC. This independent evaluation was prepared based on information available as of September 30, 2017.

Methodology

We conducted component level and system level testing to support compliance with FISMA. The following were reviewed in support of the audit:

- Organizational responsibilities and authority
- Information security policies and procedures
- System security plans
- Risk assessments
- Continuity of operations plan
- Security incident reporting
- Security awareness, training, and education
- Security assessment and authorization

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

- Remedial action process (plan of action and milestones)
- System configuration management
- Annual information security program reporting

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 Officers Act audits.

In addition, we assessed PBGC's technical controls by performing a network security test as part of the FISMA independent evaluation. The independent vulnerability assessment and penetration test was conducted to determine the effectiveness of internal controls that prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the vulnerability assessment and penetration test was incorporated into our FISMA evaluation results. Evaluation procedures included reviewing policies and procedures, interviewing employees and contractors, reviewing and analyzing records, and reviewing supporting documentation. PBGC OIG provided oversight of the evaluation team's performance.

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Appendix B: Status of Prior-Year Recommendations

The following is the status of outstanding recommendations not included in the report and PBGC's plans for corrective action. As noted in the table below, some recommendations remain in progress, with estimated completion dates still to be determined. The corrective actions outlined below are based on management assertions and results of our evaluation.

FISMA Recommendations Closed in Fiscal Year 2017

OIG Control Number	Date Closed	Original Report Number
FISMA-15-03	11/07/17	EVAL 2016-7/FA-15-108-7
FISMA-15-04	11/02/17	EVAL 2016-7/FA-15-108-7
FISMA-15-07	11/02/17	EVAL 2016-7/FA-15-108-7
FISMA-15-08	11/13/17	EVAL 2016-7/FA-15-108-7
FISMA-16-01	11/07/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-02	11/07/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-06	11/02/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-07	11/07/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-09	10/23/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-13	11/13/17	EVAL 2017-9 /FA-16-110-7
FISMA-16-20	11/06/17	EVAL 2017-9 /FA-16-110-7

Prior and Current Years' Open FISMA Recommendations in Fiscal Year 2017

OIG Control Number	Original Report Number
<i>Prior Year</i>	
FISMA-14-15	EVAL 2015-9/FA-14-101-7
FISMA-15-01	EVAL 2016-7/FA-15-108-7
FISMA-15-02	EVAL 2016-7/FA-15-108-7
FISMA-15-05	EVAL 2016-7/FA-15-108-7
FS-07-17	AUD-2009-2/FA-08-49-2
FS-14-12	AUD-2015-3/FA-14-101-3
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-16-08	EVAL 2017-9 /FA-16-110-7
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-16-14	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

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

OIG Control Number	Original Report Number
<i>Current Year</i>	
FS-15-04	AUD 2016-3/FA-15-108-3
FISMA-17-01	
FISMA-17-02	
FISMA-17-03	
FISMA-17-04	

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

Appendix C: Management Comments




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

Office of the Director

DEC 12 2017

To: Robert A. Westbrooks
Inspector General

From: W. Thomas Reeder 

Subject: Response to OIG's Draft Fiscal Year 2017 FISMA Report

Thank you for the opportunity to comment on the Office of Inspector General (OIG's) draft report, dated December 4, 2017, relating to FY 2017 compliance with the Federal Information Security Management Act (FISMA). Your office's work on this is sincerely appreciated.

It was helpful to receive the associated Notices of Findings and Recommendations (NFRs) 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.

Management is in agreement with the report's findings and recommendations. In the attachment to this report, you will find 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, 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

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

ATTACHMENT

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

1. FISMA-17-01 Revise process and procedures to ensure the continuous monitoring program is consistently enforcing the review, update, and uploading of all required security assessment and authorization documentation for each system before the documentation expires. (*NFR 17-09*)

PBGC Response:

PBGC agrees with this recommendation. The following corrective actions will be taken in response to this recommendation: PBGC will consistently conduct reviews to ensure required system security documentation is approved, updated and uploaded in Cyber Security Assessment and Management (CSAM). A Plan of Action and Milestones (POA&M) will be created to address the recommendation and support Cybersecurity program maturity.

Scheduled Completion Date: June 30, 2018

2. FISMA-17-02 Complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4, revise the inheritance of common controls, and conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4. (*NFR 17-10*)

PBGC Response: PBGC agrees with this recommendation. The corporation will complete the update of control implementation statements during FY18 with accomplishments officially identified through quarterly Security and Privacy Assessment and Authorization (SPA&A) reporting conducted by PBGC's Enterprise Cybersecurity Department.

Scheduled Completion Date: September 30, 2018

3. FISMA-17-03 Document and implement enhanced process and procedures to effectively track and remediate known vulnerabilities in a timely manner. (*NFR 17-08*)

PBGC Response: PBGC concurs with this recommendation. The corporation is currently reviewing its vulnerability tracking and remediation process to determine what process enhancements can be made to more effectively track known vulnerabilities. PBGC will determine its implementation strategy and timing following the completion of the process review based on available funding and resources.

Scheduled Completion Date: June 30, 2018

**PENSION BENEFIT GUARANTY CORPORATION
FY 2017 FISMA EVALUATION**

4. FISMA-17-04 PBGC should implement effective process and procedures to ensure the secure configuration of web servers in accordance with the established configuration baselines and document deviations to the established baselines on an as needed basis. *(NFR 17-11)*

PBGC Response: PBGC concurs with this recommendation and takes the security of its information systems seriously. The corporation previously developed secure configuration baselines for web servers and deployed a configuration checklist within its endpoint management and security solution. However, PBGC recognizes more improvement is needed in this area. PBGC has already developed and begun to implement a Plan of Action and Milestones (POA&M) to address this finding and improve the operational effectiveness of its configuration management controls.

Scheduled Completion Date: July 31, 2018

5. FS-15-04 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.

PBGC Response:

PBGC agrees with this recommendation. The following corrective actions will be taken in response to this recommendation: PBGC will consistently review, approve, update and upload required system security documentation in Cyber Security Assessment and Management (CSAM). A Plan of Action and Milestones (POA&M) will be created to address the recommendation and support Cybersecurity program maturity.

Scheduled Completion Date: June 30, 2018