OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

Fiscal Year 2025 Pension Benefit Guaranty Corporation Federal Information Security Modernization Act of 2014 (FISMA) Independent Performance Audit

Report No. AUD-2025-12
September 30, 2025

September 30, 2025

MEMORANDUM

TO: Alice Maroni
Acting Director

Robert Scherer
Chief Information Officer

FROM: Nicholas J. Novak
Inspector General

Nicholas J. Novak

SUBJECT: Fiscal Year 2025 Pension Benefit Guaranty Corporation Federal Information Security Modernization Act of 2014 (FISMA) Independent Performance Audit (AUD-2025-12)

I am pleased to transmit the results of our Fiscal Year 2025 Pension Benefit Guaranty Corporation FISMA Independent Performance Audit. As prescribed by FISMA, the Inspector General is required to conduct an annual assessment of PBGC's security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this audit.

KPMG LLP, our independent auditor, completed the Inspector General FISMA metrics submitted to OMB. This year, our independent auditor found PBGC's information security programs and practices effective. However, weaknesses were identified in the risk and asset management and incident response domains. PBGC concurred with the report's findings and four recommendations.

cc: Joshua Kossoy
Tim Hurr
Arrie Etheridge
Karen Morris
Lisa Carter
John Hanley
David Foley
Michael Rae
Steve Young

Fiscal Year 2025 Pension Benefit Guaranty Corporation Federal Information Security Modernization Act of 2014 (FISMA) Independent Performance Audit

September 29, 2025

kpmg.com

KPMG LLP
1051 East Cary Street
Suite 900
Richmond, VA 23219-4023

September 29, 2025

Mr. Robert Scherer
Chief Information Officer
Pension Benefit Guaranty Corporation
445 12th Street SW
Washington, DC 20024-2101

Mr. John Seger
Assistant Inspector General for Audits
Pension Benefit Guaranty Corporation
445 12th Street SW
Washington, DC 20024-2101

Dear Mr. John Seger and Mr. Robert Scherer,

This report presents the results of our independent performance audit of the Pension Benefit Guaranty Corporation (PBGC) information security program and practices for its information systems. We conducted our performance audit from March 12, 2025, through July 31, 2025, and our results are through the period of October 1, 2024, through June 30, 2025.

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

In addition to GAGAS, we conducted this performance audit in accordance with the Consulting Services Standards established by the American Institute of Certified Public Accountants (AICPA). This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), the objectives of this performance audit were to:

- Report on the effectiveness of PBGC's information security program and practices for FY 2025 using outputs calculated by the CyberScope reporting tool. Specifically, we tested the design and the operating effectiveness of relevant information security controls from October 1, 2024 through June 30, 2025.
- Conduct the performance audit in accordance with the FISMA, Office of Management and Budget (OMB) *Guidance on Federal Information Security and Privacy Management Requirements*, Government Accountability Office GAGAS, AICPA Consulting Standards, and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0.
- Follow up on the status of prior-year FISMA performance audit findings.

KPMG cautions that projecting the results of our performance audit to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

This report is intended solely for the use of PBGC, the PBGC Office of Inspector General (OIG), Department of Homeland Security (DHS), Government Accountability Office, and OMB and is not intended to be and should not be relied upon by anyone other than these specified parties.

KPMG LLP

September 29, 2025

Table of Contents

Background 2

Overall Results 9

Metric Domain Results 10

Govern 10

Cybersecurity Governance 10

Cybersecurity Supply Chain Risk Management 11

Identify 11

Risk Management 11

Protect 12

Configuration Management 12

Identity and Access Management 12

Data Protection and Privacy 13

Security Training 13

Detect – Information Security Continuous Monitoring 13

Respond – Incident Response 14

Recover – Contingency Planning 14

Audit Recommendations and Findings 16

Identify – RM – Risk Assessments 16

Recover – CP – Lack of a Contingency Plan 17

Conclusion 19

Appendix I: Glossary of Terms 20

Appendix II: Status of Prior Recommendations 21

Appendix III: Management's Response to the Audit Report 22

Background

KPMG LLP (KPMG) performed the fiscal year (FY) 2025 independent Federal Information Security Modernization Act of 2014 (FISMA) audit, under contract with and on behalf of PBGC Office of Inspector General (OIG), as a performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Consulting Standards established by the American Institute of Certified Public Accountants (AICPA). PBGC OIG monitored our work to ensure that we met professional standards and contractual requirements.

Agency Overview

PBGC (or the Corporation) is a federal corporation established under the Employee Retirement Income Security Act of 1974 (ERISA). Congress established PBGC to insure the pension benefits of workers and retirees. ERISA Section 4002(a)[1] describes the following its purposes, which are to be carried out by PBGC:

- Encourage the continuation and maintenance of voluntary private pension plans for the benefit of their participants.
- Provide for the timely and uninterrupted payment of pension benefits to participants and beneficiaries under plans to which this title applies.
- Maintain premiums established by the Corporation under ERISA Section 4006 at the lowest level consistent with carrying out its obligations under ERISA Title IV.[2]

Federal Information Security Modernization Act of 2014

On December 17, 2002, the President signed FISMA[3] into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). The purpose of this act was to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets and provide a mechanism for improved oversight of federal agency information security programs. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendment (1) included the reestablishment of 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 the authority for the Secretary of the Department of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. FISMA requires that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including assessing the risks and magnitude of the

---

[1] ERISA, available at: https://www.govinfo.gov/content/pkg/COMPS-896/pdf/COMPS-896.pdf, accessed on August 21, 2025

[2] PBGC Strategic Plan FY 2022-2026, available at: https://www.pbgc.gov/sites/default/files/documents/pbgc-fy-2022-2026-strategic-plan.pdf, accessed on August 21, 2025

[3] Federal Information Security Management Act of 2002 (FISMA), Pub. L. No.107-347, tit. III, Section 301, Subsection 3544(a)(1)(A), Dec. 17, 2002, available at: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf, accessed on August 21, 2025

harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems.

FY 2025 IG FISMA Reporting Metrics

OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), with review and feedback provided by several stakeholders, including the Federal Chief Information Officers and Chief Information Security Officers councils, released OMB's guidance for implementing the requirements outlined in OMB Memorandum (M) 25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements,* outlined in the *FY 2025 Inspector General FISMA Reporting Metrics* ("FY 2025 IG Metrics"). The FY 2025 IG Metrics are aligned with the six information security functions outlined in the *National Institute of Standards and Technology* (*NIST) Framework for Improving Critical Infrastructure Cybersecurity* ("NIST Cybersecurity Framework"): Govern, Identify, Protect, Detect, Respond, and Recover. CIGIE maintained the maturity models for the following 10 FISMA Metric Domains: Cybersecurity Governance (CG), Cybersecurity Supply Chain Risk Management (C-SCRM), Risk and Asset Management (RAM), Configuration Management (CM), Identity and Access Management (IDAM), Data Protection and Privacy (DPP), Security Training (ST), Information Security Continuous Monitoring (ISCM), Incident Response (IR), and Contingency Planning (CP). **Table 1** illustrates the alignment of NIST Cybersecurity Framework to the FISMA Metric Domains within the FY 2025 IG Metrics.

Table 1: Alignment of NIST Cybersecurity Framework to the FISMA Metric Domains

Cybersecurity Framework Functions	FISMA Metric Domains
Govern	Cybersecurity Governance Cybersecurity Supply Chain Risk Management
Identify	Risk and Asset Management
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Consistent with FY 2024, the model has five maturity levels: *Ad hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. **Table 2** details the five maturity levels to assess the agency's information security program for each Cybersecurity Function.

Table 2: Inspector General Assessed Maturity Levels

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, and regularly updated based on a changing threat and technology landscape and business/mission needs.

The FY 2025 IG Metrics included the removal of each Supplemental Metric from the FY 2023-FY 2024 IG FISMA Metrics. The FY 2025 IG Metrics still include both Core and Supplemental Metrics; however, the Supplemental Metrics were tailored to the Administration's priorities. The FY 2025 IG Metrics included Core Metrics and Supplemental Metrics, as depicted in **Table 3.**

Table 3: FY 2025 Metric Scoping

Core Metrics	Supplemental Metrics
5 - SCRM Processes	1 - Agency Cybersecurity Profiles
7 - System Inventory	2 - Cybersecurity Risk Management Strategy
8 - Hardware Inventory	3 - Cybersecurity Roles and Responsibilities
9 - Software Inventory	10 - Data Inventory
11 - Enterprise Risk Management & Risk Assessments	15 - Data Inventory
12 - Risk Management Dashboards and Reporting	27 - System Integrity and Security Posture Monitoring
14 - Configuration Settings	
15 - Flaw Remediation	
17 - Multi-factor Authentication - General Users	
18 – Multi-factor Authentication - Privileged Users	
19 - Privileged User Account Management	
21 - Encryption	
22 - Data Exfiltration and Network Defenses	
24 - Workforce Assessment	
26 - ISCM Strategy	
28 - ISCM Processes	
30 - Incident Response Tools and Detection	
31 - Incident Response Tools and Handling	
33 - Business Impact Analysis	
34 - Information System Contingency Plan Test, Training, and Exercise	

IG FISMA Reporting Metrics Scoring

According to the FY 2025 IG Metrics guidance, a security program is considered effective if the calculated average of the Metrics in a particular Domain is *Managed and Measurable* (Level 4) or higher. For FY 2025, a calculated average scoring model was used in which Core Metrics and Supplemental Metrics were averaged independently to determine a Domain's maturity calculation and provide data points for the assessed program and function effectiveness. The calculated averages of both the Core Metrics and Supplemental Metrics were used as a data point to support the risk-based determination of overall program and function level effectiveness.

In addition to the calculated average, the FY 2025 IG Metrics introduced a weighted average as a pilot in FY 2025. OMB and CIGIE selected eight metrics that were determined to have a greater importance towards achieving cybersecurity effectiveness. These metrics were chosen to be

"Foundational Metrics." Cyberscope[4] calculated Foundational Metrics to have double the weight of "Non-Foundational Metrics" when calculating the average rating for each Metric Domain, Function, and the overall rating. OIGs had the discretion to consider the weighted average as a data point in their effectiveness determinations.

Other data points considered included:

- The results of cybersecurity evaluations, including system security control reviews, vulnerability scanning, and penetration testing conducted during the period October 1, 2024 through June 30, 2025 ("the audit scope period");
- The progress made by agencies in addressing outstanding Inspector General (IG) recommendations; and
- Reported security incidents reported during the audit scope period.

FY 2025 IG Metrics establish that IGs should use the CyberScope reporting tool to calculate and submit the maturity levels for each Cybersecurity Function and Domain to DHS and OMB. CyberScope provides supplementary fields to allow explanatory comments; IGs may use these fields to provide additional data supporting the Core Metrics evaluation results, and ultimately provide the overall effectiveness of the PBGC's information security program.

Objective, Scope, and Methodology

Objective

In accordance with the FISMA, the objectives of this performance audit were to:

- Report on the effectiveness of PBGC's information security program and practices for FY 2025 using outputs calculated by the CyberScope reporting tool. Specifically, we tested the design and the operating effectiveness of relevant information security controls from October 1, 2024 through June 30, 2025.
- Conduct the performance audit in accordance with the FISMA, OMB Guidance on Federal Information Security and Privacy Management Requirements, Government Accountability Office GAGAS, AICPA Consulting Standards, and the NIST Cybersecurity Framework (CSF) 2.0.
- Follow up on the status of prior-year FISMA performance audit findings.

Scope

To accomplish our objectives, we evaluated security controls in accordance with applicable legislation; FY 2025 IG Metrics; applicable NIST standards and guidelines, presidential

[4] CyberScope, operated by DHS on behalf of OMB, is a web-based application designed to streamline information technology security reporting for Federal agencies. It gathers and standardizes data from Federal agencies to support FISMA compliance. In addition, Offices of Inspectors General provide an independent assessment of effectiveness of an agency's information security program. Offices of Inspectors General must also report their results to DHS and OMB annually through CyberScope.

directives, and OMB memorandums referenced in the FY 2025 IG Metrics; and PBGC policies and procedures. We performed procedures to assess whether selected controls established by PBGC's information security program were designed, implemented, and operating effectively from both an entity-wide and system-level perspective.

We selected eight information systems (four PBGC-operated and four contractor-operated information systems) that support the Corporation to perform system-level testing and determine whether select security controls were suitably designed, implemented, and operating effectively during the audit scope period.

Methodology

We conducted this performance audit in accordance with GAGAS, which requires that we plan and conduct this performance 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. In addition to GAGAS, we conducted this performance audit in accordance with Consulting Services Standards established by the AICPA. This performance audit did not constitute an audit of financial statements or an attestation level report as defined under GAGAS and the AICPA standards for attestation engagements.

We requested that PBGC management provide a self-assessment of maturity levels for the FY 2025 IG Metrics to help us gain a better understanding of how the organization implemented relevant security controls and processes for the 26 metrics in scope. The Corporation described policies, procedures, and controls relevant to each metric in the self-assessment provided to us for inspection, which assisted us in requesting appropriate artifacts and meetings so that we could perform our audit procedures and conduct an independent assessment of the maturity levels.

Our procedures to assess the effectiveness of PBGC's information security program and practices included the following:

- Inquiry of PBGC Information System Owners (ISOs), Information Owners (IOs), Information System Security and Privacy Officers (ISSPOs), system administrators, and other relevant control operators to walk through control processes applicable to each metric.
- Walkthroughs and observations of live of cybersecurity processes and controls.
- Inspection of PBGC information security policies, procedures, and guidelines established and disseminated by PBGC Office of Information Technology.
- Inspection and observation of client artifacts in order to determine whether PBGC processes and controls applicable to each metric were designed, implemented, and operating effectively across the Corporation and for the selected information systems during the audit.

We conducted our field work from March 12, 2025, through July 31, 2025. We also periodically met with PBGC management and the PBGC OIG to discuss our audit progress and identified findings.

Criteria

We designed the approach for conducting our FISMA performance audit in consideration of Federal information security guidance developed by NIST and OMB. NIST Special Publications (SP) provide guidelines associated with the development and implementation of agencies' security programs. We also leveraged a variety of PBGC directives, manuals, standard operating procedures, and other system-level guidance for information security. For each finding detailed in the Audit Findings and Recommendations section of this report, we included the relevant PBGC, OMB, and/or NIST criteria.

Overall Results

Consistent with the FISMA requirements, OMB policy and guidance, and NIST standards and guidance, PBGC established and maintained its information security program and practices for the 6 Cybersecurity Functions and 10 FISMA Metric Domains. In this report, we included 2 findings noted within 2 of the 6 FISMA Cybersecurity Functions (Identify and Recover) and 2 of the 10 FISMA Metric Domains (RAM and CP). We made four recommendations related to these findings that, if effectively implemented, should strengthen PBGC's information security program.

As a result of our performance audit, we assessed PBGC's information security program as *Managed and Measurable* (Level 4), which reflects an effective information security program overall according to the FY 2025 IG Metrics guidance. **Table 4** below depicts PBGC's maturity levels for the six Cybersecurity Functions.

Table 4: Maturity Levels for Cybersecurity Functions

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
1. Govern Cyber Governance Cybersecurity-Supply Chain Risk Management	*1. Govern: Level 4: Managed and Measurable* CG – Level 4: Managed and Measurable C-SCRM – Level 4: *Managed and Measurable*
2. Identify Risk and Asset Management	*2. Identify: Level 4: Managed and Measurable* RAM – Level 4: Managed and Measurable
3. Protect Configuration Management Identity Access Management Data Protection and Privacy Security Training	*3. Protect: Level 4: Managed and Measurable* CM – Level 4: Managed and Measurable IDAM – Level 4: Managed and Measurable DPP – Level 4: Managed and Measurable ST – Level 4: Managed and Measurable
4. Detect Information Security Continuous Monitoring	*4. Detect: Level 4: Managed and Measurable* ISCM – Level 4: Managed and Measurable
5. Respond Incident Response	*5. Respond: Level 4: Managed and Measurable* IR – Level 4: Managed and Measurable

Cybersecurity Framework Functions & FISMA Metric Domain Areas	Maturity Level
6. Recover Contingency Planning	*6. Recover: Level 4: Managed and Measurable* CP – Level 4: *Managed and Measurable*
Overall Maturity Level	**Level 4: Managed and Measurable**
Overall Effectiveness	**Effective**

Metric Domain Results

For each Metric Domain, we have summarized our results related to our testing and our rationale for our assessed maturity level and included any findings identified for the related Metric Domains in the sections that follow.

Govern

The Govern Function informs an organization as to measures it may take to prioritize and achieve the outcomes of the other five Functions in the context of its mission and stakeholder expectations.[5] Within the Govern Function, there are two Cybersecurity Domains: CG and C-SCRM.

Cybersecurity Governance

Cybersecurity governance is defined by the NIST Cybersecurity Framework as a comprehensive strategy that integrates with organizational operations and prevents the interruption of activities due to cyber threats or attacks.[6] Strong governance aligns an organization's cybersecurity activities with its business objectives, legal and regulatory requirements, and risk management strategies.

Based on the results of our audit procedures, we determined that PBGC developed and maintained current and target cybersecurity profiles. PBGC implemented its risk management strategy at the organizational, office, and system levels. PBGC consistently evaluated and adjusted its cybersecurity risk management strategy based on its threat environment and organization-wide cyber and privacy risk assessment. Additionally, PBGC used qualitative and quantitative data to assess cybersecurity risk management effectiveness. Finally, PBGC allocated resources commensurate with the cybersecurity risk strategy, roles, responsibilities, policies, and profiles.

[5] NIST Cybersecurity Framework 2.0, available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf, accessed on August 21, 2025

[6] As defined by the Cybersecurity and Infrastructure Security Agency, available at: https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance, accessed on August 21, 2025

Cybersecurity Supply Chain Risk Management

C-SCRM requires agencies to develop policies, procedures, and programs to manage supply chain risks associated with system development, acquisition, maintenance, and disposal. This includes monitoring third-party vendors and service providers and helping to ensure appropriate contractual requirements are included for acquisitions.

Based on the results of our performance audit procedures, we determined that PBGC obtained sufficient assurance that the security and supply chain controls of systems or services provided by contractors or other entities on behalf of PBGC meet FISMA requirements, OMB policy, and applicable NIST guidance. PBGC analyzed its suppliers through a holistic view of risk through cybersecurity posture assessments and through the use of digital threat intelligence.

Identify

The NIST Cybersecurity Framework identifies the objective of the Identify Function as understanding and managing cybersecurity risks to systems, people, assets, data, and capabilities within an organization. Understanding cybersecurity risks enables an agency to focus and prioritize efforts consistent with its risk management strategy and business needs.

Risk Management

FISMA requires federal agencies to establish an information security program that protects the systems, data, and assets from various threats and risks commensurate with their risk environment. These threats or risks could stem from various sources, including budget uncertainty, natural disasters, and cybersecurity incidents. A sound risk management plan and program that addresses relevant risks and threats can aid an agency in establishing an information security program.

Based on the results of our audit procedures, we determined that PBGC implemented policies and procedures to maintain a complete and accurate inventory of its major information systems by using a Governance, Risk, and Compliance platform to store and manage system security information. PBGC used a configuration management database integrated with its asset discovery tools to create and maintain a near real-time hardware and software database. PBGC consistently monitored the effectiveness of risk responses to help ensure that risk tolerances were maintained at an appropriate level. Cybersecurity risks were quantified, aggregated, and normalized across each office and the corporation and prioritized accordingly.

However, we identified two information systems that did not update their risk assessments within the past year as required by PBGC policy. Although PBGC management self-identified the deficiency, they failed to establish a Plan of Action and Milestones (POA&M) within 30 days of identifying the weakness as required by PBGC policy.

Protect

The NIST Cybersecurity Framework identifies the objective of the Protect Function as developing and implementing appropriate safeguards to enable the delivery of critical services of organizations. The Protect Function supports organizations' ability to limit, contain, or prevent the impact of a cybersecurity event. This Function includes the CM, IDAM, DPP, and ST cybersecurity domains.

Configuration Management

FISMA requires agencies to develop an information security program that includes policies and procedures that enable compliance with minimally acceptable system configuration requirements. CM refers to a collection of activities focused on establishing and maintaining the integrity of information systems and related products through the control of processes for initializing, changing, and monitoring their configurations.

Based on the results of our audit procedures, we determined that PBGC employed automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for its information system components connected to its network and made appropriate modifications in accordance with PBGC-defined timelines. Components that failed to meet the PBGC-defined timelines were automatically removed from the network.

PBGC centrally managed its flaw remediation process and used automated patch management and software update tools for operating systems. PBGC's Patch Vulnerability Management Group analyzed quantitative and qualitative performance measures to track remediation and enforce PBGC required timelines for remediation of vulnerabilities. Furthermore, PBGC used software code scanning to secure code early in the development process.

Identity and Access Management

IDAM requirements dictate that agencies implement capabilities to help ensure that information system users can only access data required for their job functions in accordance with the principles of separation of duties and least privilege. Aspects of the IDAM program include screening personnel, issuing and maintaining user credentials, and managing logical and physical access rights.

Based on the results of our audit procedures, we determined that PBGC utilized strong authentication mechanisms to authenticate to information systems integrated, to the extent possible, with a centralized enterprise identity management system. Privileged access was monitored employing a privileged access management tool that tracked all use of privileged accounts to help ensure compliance with PBGC policies.

Data Protection and Privacy

DPP refers to a collection of activities focused on the security objective of confidentiality, the preservation of authorized restrictions of information access, and the protection against improper disclosure of personal privacy and proprietary information. Effectively managing the risks associated with the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of personally identifiable information (PII) increasingly depends on the safeguards employed for systems that process, store, and transmit such information. Accordingly, OMB Circular A-130[7] requires federal agencies to develop, implement, and maintain agency-wide privacy programs that, where PII is involved, play a key role in information security and the proper implementation of the NIST Risk Management Framework. Although the head of each federal agency remains ultimately responsible for ensuring privacy interests are protected and PII is managed responsibly, Executive Order 13719[8] requires agency heads to designate a Senior Agency Official for Privacy who is accountable for the agency's privacy program.

Based on the results of our audit procedures, we determined that PBGC implemented security controls to protect PII and other sensitive agency data, and those controls were subject to monitoring processes defined within the PBGC ISCM strategy. PBGC conducted data exfiltration exercises to measure the effectiveness of its data exfiltration detection and enhanced network defenses.

Security Training

ST is a cornerstone of a strong information security program as regular users and privileged users must have the knowledge to perform their jobs appropriately while using information system resources without exposing the organization to unnecessary risk.

Based on the results of our audit procedures, we determined that PBGC assessed the knowledge, skills, and abilities of its workforce; tailored its specialized training; and addressed identified skill gaps.

Detect – Information Security Continuous Monitoring

The NIST Cybersecurity Framework defines the objective of the Detect Function as the timely discovery of cybersecurity events. This function is critical to maintaining a robust information security program as the effects of cybersecurity events can be mitigated more quickly if they are identified in a timely manner. The NIST Cybersecurity Framework states that ISCM processes should be used to detect anomalies and continuously monitor information systems across the

---

[7] OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016), available at: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf, accessed on August 21, 2025

[8] Executive Order 13719, Establishment of the Federal Privacy Council, issued February 9, 2016, available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council, accessed on August 21, 2025

enterprise to identify events. The Detect Function is carried out through the effective configuration and use of ISCM tools and processes intended to promote timely identification of cybersecurity events.

Based on the results of our audit procedures, we determined that PBGC management implemented an enterprise-wide Security Information Event Management platform. PBGC ingested data from its end points and service providers, analyzed the data and delivered key performance measures to appropriate stakeholders. Further, PBGC evaluated its continuous monitoring activities throughout the year for effectiveness, and an annual report was published highlighting PBGC's cybersecurity posture, successes, and areas for improvement. Where appropriate, PBGC employed ongoing authorization and performed annual Security and Privacy Assessment and Authorization (SPA&A) reviews of each system included in the scope of our performance audit to help ensure compliance with the PBGC security authorization program.

Respond – Incident Response

The NIST Cybersecurity Framework defines the objective of the Respond Function as the development and implementation of actions taken upon detection of a cybersecurity event. Such actions include the establishment of proper IR plans and procedures to be executed during and after incidents, analysis to determine the impact of incidents and mitigation to contain and resolve incidents, managing communications with relevant stakeholders during and after incidents, and incorporating lessons learned into the IR program. Executive Order (EO) 14028 requires Federal Civilian Executive Branch Agencies to document and implement an IR program following operational procedures defined by the Cybersecurity and Infrastructure Security Agency.

Based on the results of our audit procedures, we determined that PBGC management implemented an effective IR program through the execution of security incident management (SIM) plans, procedures, and playbooks and the use of advanced IR tools. These tools offered PBGC a centralized view of incident response activities on a near real-time basis as well as timely containment and resolution of incidents. The PBGC-Computer Emergency Response Team established SIM rules of engagement to quickly analyze and respond to cybersecurity incidents while not disrupting operations.

Recover – Contingency Planning

The NIST Cybersecurity Framework defines the objective of the Recover Function as the maintenance of plans for resilience and restoration of any capabilities or services impaired due to a cybersecurity incident or other disaster. Activities that are part of this function, such as developing and testing contingency plans, support timely recovery to normal operations and reduce the impact from an incident or disaster.

Based on the results of our audit procedures, we determined that PBGC management identified its critical business functions through the use of a corporation Business Impact Analysis(BIA), which was integrated into and used to inform system BIAs. Additionally, PBGC configured its infrastructure with geo-redundant capabilities and disaster recovery as a service to minimize outages. Furthermore, PBGC performed biannual CP exercises including an annual failover and failback test of applications and workloads.

However, for one of eight information systems selected for testing, we determined that management did not create and maintain a contingency plan.

Audit Recommendations and Findings

The following sections provide a summary of the audit recommendations and findings for each of the FISMA Metric Domains required to be monitored under FISMA. We did not identify any new findings or recommendations for the CG, C-SCRM, DPP, ST, ISCM, and IR FISMA Metric Domains and have, therefore, omitted them from this section.

Identify – RM – Risk Assessments

PBGC management did not update its risk assessments for two of eight systems selected for testing as required by the Information Security Risk Management Framework Process guidance. Specifically, the risk assessment for one system was reviewed on June 12, 2025, which was 933 days later than the PBGC policy required, and the other system's risk assessment review was last completed on August 8, 2023, with no updates made as of July 31, 2025. Despite PBGC management identifying the failure to update these risk assessments as a deficiency during Security and Privacy Assessment and Authorization (SPA&A) reviews, a POA&M was not established and tracked in accordance with enterprise policy, which mandates the creation of a POA&M within 30 days of identifying a weakness.

Information Security Risk Management Framework (RMF) Process, Version 4.5, dated May 2025, states:

> *Proper risk management requires steps to be taken to reduce the risk level to an acceptable level. A team led by the ISSPO and the ISSPO or ISO/IO designee should perform a [risk assessment] for all new systems and systems undergoing major modification or migrating into a new boundary. For existing information systems that have not undergone any significant changes, an annual review of the system level [risk assessment] is required.*

Enterprise Plan of Action and Milestone (POA&M) Process, Version 5.5, dated May 2025, states:

> *Security and privacy weaknesses that will require more than 30 days to resolve must be entered in [Cyber Security Assessment and Management] as soon as possible and within 30 days of identification, with estimated completion dates for each milestone and an overall completion date for the POA&M.*

The two system's risk assessments were not updated timely because the ISSPO and ISO were unaware of the requirement to review the risk assessment on an annual basis. The failure to record a POA&M related to the delayed risk assessments for the two systems occurred because the transition of the ISSPO role was not managed effectively. Specifically, the SPA&A results were not communicated to the ISSPO, leaving them unaware of the existing control deficiency.

When a system's risk assessment is not updated, the identification of threats, assessment of vulnerabilities, and estimation of the likelihood that a threat could exploit those vulnerabilities become outdated and potentially inaccurate. This increases the risk that PBGC's risk responses no longer reduce risk related to the system to an acceptable level.

Failure to timely create, monitor, and execute POA&Ms for identified security deficiencies increases the risk of unresolved vulnerabilities within the organization's information systems. This can lead to potential unauthorized access, data breaches, and non-compliance with regulatory requirements, thereby compromising the confidentiality, integrity, and availability of critical data and systems.

Recommendations:

We recommend PBGC management:

- Provide training to ISSPOs, ISOs, and Information Owners on their roles and responsibilities to follow the PBGC RMF and POA&M processes (**Recommendation 2025-12-01**),
- Confirm the requirement that deficiencies identified by SPA&A reviews that are not remediated within 30 days after identification are tracked via POA&Ms with accountable personnel (**Recommendation 2025-12-02**), and
- Periodically monitor the satisfaction of the system risk assessment and POA&M creation requirements to help ensure ongoing compliance associated with the timely completion of and updates to system risk assessments and documentation and tracking of POA&Ms. (**Recommendation 2025-12-03**)

Recover – CP – Lack of a Contingency Plan

PBGC management did not create and maintain a contingency plan for one of eight systems selected for testing.

Information System Contingency Plan (ISCP) Process, Version 1.3, dated March 2025, states:

> *If another Federal Agency, a contractor, or vendor hired by PBGC is responsible for the Contingency Planning controls, the third party should implement the contingency plan and perform the contingency plan test including the applications and information owned…To receive an [Authority to Operate], systems must complete their CP plan and conduct a CP test. The CP test should be consistent with the system categorization.*

The system was hosted by a cloud service provider (CSP); however, ambiguities in PBGC and the CSP's service agreement and responsibility matrix led to the incorrect assumption that development and maintenance of the contingency plan were the CSP's sole responsibility.

Without a contingency plan, PBGC may be unable to respond effectively to an incident or system disruption, delaying the restoration of operations. This increases the risk the system will not meet its recovery time objective or recovery point objective.

Recommendations:

We recommend PBGC management to coordinate with its CSP to update its service agreement and shared responsibility matrix to address ambiguities regarding accountable parties for key controls and develop and implement a contingency plan for the system (**Recommendation 2025-12-04**).

Conclusion

Based on the results of our performance audit procedures, we conclude that PBGC management established and maintained its information security program and practices for its information systems for the six Cybersecurity Functions and ten FISMA Metric Domains during FY 2025. We assessed PBGC's information security program as "Effective" within CyberScope, as the majority of the FY 2025 IG Metrics and the associated calculated averages for the Metric Domains and Cybersecurity Functions were assessed at a maturity of Level 4 (Managed and Measurable). Specifically, the Govern, Identify, Protect, Detect, Respond, and Recover Cybersecurity Functions were assessed as "Managed and Measurable". We also performed follow-up testing to determine the status of the seven prior year recommendations and report that six of the seven recommendations were closed (see **Appendix II**). As a result of procedures performed, we determined that one prior year recommendation remained open[9] and also reported two new findings that impacted the Identify and Recover Cybersecurity Functions.

We made four recommendations related to the two new findings that should strengthen PBGC's information security program if effectively addressed by management. PBGC management should consider whether these recommendations apply to other information systems maintained in the organization's FISMA system inventory and implement remedial action as needed. In a written response, PBGC agrees with our findings and recommendations for strengthening their information security program (see **Appendix III**).

[9] The open recommendation was not scheduled to be implemented until December 31, 2025.

Appendix I: Glossary of Terms

AICPA	American Institute of Certified Public Accountants
BIA	Business Impact Analysis
Corporation	Pension Benefit Guaranty Corporation
CG	Cybersecurity Governance
CIGIE	Council of Inspectors General on Integrity and Efficiency
CM	Configuration Management
CP	Contingency Planning
CSF	Cybersecurity Framework
CSP	Cloud Service Provider
C-SCRM	Cybersecurity Supply Chain Risk Management
DHS	Department of Homeland Security
DPP	Data Protection and Privacy
EO	Executive Order
ERISA	Employee Retirement Income Security Act of 1974
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal year
FY 2025 IG Metrics	FY 2025 Inspector General FISMA Reporting Metrics
GAGAS	Generally Accepted Government Auditing Standards
IDAM	Identity and Access Management
IG	Inspector General
IO	Information Owner
IR	Incident Response
ISCM	Information System Continuous Monitoring
ISCP	Information System Contingency Plan
ISO	Information System Owner
ISSPO	Information System Security and Privacy Officer
KPMG LLP	KPMG
M	Memorandum
NIST	National Institute of Standards and Technology
NIST Cybersecurity Framework	National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
OIG	Office of Inspector General
OMB	Office of Management and Budget
PBGC	Pension Benefit Guaranty Corporation
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
RAM	Risk and Asset management
RMF	Risk Management Framework
SIM	Security Incident Management
SP	Special Publication
SPA&A	Security and Privacy Assessment and Authorization
ST	Security Training

Appendix II: Status of Prior Recommendations

As part of the FY 2025 FISMA Performance Audit, we performed procedures to determine whether management closed prior year recommendations. Recommendations were closed if management provided sufficient documentation to evidence that the associated recommendations were fully implemented. Findings with recommendations that were determined not to be completely implemented remained open. As outlined in **Table 5** below, we determined that six of seven prior year recommendations were closed. One of seven prior year recommendations has a scheduled completion date of December 31, 2025.

Table 5: Maturity Levels for Cybersecurity Functions

OIG Control Number	Recommendation	Status
2024-06-02-OIT	Update software that is no longer supported or receiving regular security to supported versions with relevant security patches.	Closed
2025-02-01-OIT	Implement an enterprise-wide approach to prevent counterfeit components from entering its supply chain and establish performance measures to gauge the effectiveness of its anti-counterfeit policies and procedures. Additionally, PBGC should provide a comprehensive anti-counterfeit training for its personnel	Closed
2025-02-02-OIT	PBGC should manage Active Directory certificate template settings effectively by hardening and auditing existing templates in the environment. Privileges should also be assessed for all templates to prevent unauthorized changes to the configuration settings.	Closed
2025-02-03-OIT	PBGC should establish robust network segmentation and configure firewalls with default rules to ensure the guest wireless network is effectively isolated from internal resources	Closed
2025-02-04-OGC	Establish a comprehensive system for monitoring, analyzing, and reporting on quantitative performance measures to evaluate the effectiveness of its Data Breach Response policies and procedures	Open
2025-02-05-OIT	PBGC should implement an effective specialized security training program that includes steps to identify and prevent phone-based social engineering for all employees	Closed
2025-02-06-OIT	PBGC should strengthen its controls around verifying the identity of PBGC personnel prior to temporarily disabling their requirement for [Multi-Factor Authentication] MFA for remote access should a user purportedly have a malfunctioning [Personal Identity Verification] PIV card or other MFA token	Closed

Appendix III: Management's Response to the Audit Report

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

Office of the Director

September 24, 2025

MEMORANDUM

To: Nicholas J. Novak
Inspector General

From: Joshua Kossoy, ITIOD Director

JOSHUA KOSSOY
Digitally signed by JOSHUA KOSSOY
Date: 2025.09.24 08:29:45 -04'00'

Tim Hurr, Chief Information Security Officer (CISO)

Digitally signed by TIEN HURR
Date: 2025.09.24 08:47:09 -04'00'

Subject: Response to OIG's Draft Fiscal Year 2025 FISMA Report

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, relating to Pension Benefit Guaranty Corporation's Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2025. Your office's work on this is sincerely appreciated.

Management agrees with your findings and recommendations. In the attachment to this memorandum, you will find our specific responses to each non-financial statement 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 the Pension Benefit Guaranty Corporation (PBGC).

Please contact Lisa Carter should you have any questions.

cc:
Lisa Carter
Alice Maroni
David Foley
Karen Morris
Robert Scherer
Steve Young

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

1. **OIG Recommendation No. 2025-12-01: Provide training to ISSPOs, ISOs, and Information Owners on their roles and responsibilities to follow the PBGC RMF and POA&M processes.**

   PBGC Response: Management concurs with this recommendation. PBGC will provide the appropriate training to personnel regarding their roles and responsibilities in accordance with the PBGC RMF.

   Scheduled Completion Date: June 30, 2026

2. **OIG Recommendation No. 2025-12-02: Confirm the requirement that deficiencies identified by SPA&A reviews that are not remediated within 30 days after identification are tracked via POA&Ms with accountable personnel.**

   PBGC Response: Management concurs with this recommendation. PBGC will ensure that unresolved deficiencies not remediate within 30 days after identification have the appropriate POA&M response.

   Scheduled Completion Date: June 30, 2026

3. **OIG Recommendation No. 2025-12-03: Periodically monitor the satisfaction of the system risk assessment and POA&M creation requirements to help ensure ongoing compliance associated with the timely completion of and updates to system risk assessments and documentation and tracking of POA&Ms.**

   PBGC Response: Management concurs with this recommendation. PBGC will implement tracking mechanisms to ensure compliance with RMF requirements and processes.

   Scheduled Completion Date: June 30, 2026

4. **OIG Recommendation No. 2025-12-04: We recommend PBGC management to coordinate with its CSP to update its service agreement and shared responsibility matrix to address ambiguities regarding accountable parties for key controls and develop and implement a contingency plan for the system.**

   PBGC Response: Management concurs with this recommendation. PBGC will coordinate with CSPs to remove ambiguities with the implementation of key controls.

   Scheduled Completion Date: June 30, 2026