OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

Pension Benefit Guaranty Corporation's Information Security Program and Practices for Fiscal Year 2024

Report No. AUD-2025-02
October 31, 2024

Office of Inspector General

October 31, 2024

MEMORANDUM

TO: Ann Orr
Acting Director

Robert Scherer
Chief Information Officer

FROM: Nicholas J. Novak
Inspector General

Nicholas J. Novak

SUBJECT: Pension Benefit Guaranty Corporation's Information Security Program and Practices for Fiscal Year 2024 (AUD-2025-02)

I am pleased to transmit the results of our audit of Pension Benefit Guaranty Corporation’s Information Security Program and Practices for Fiscal 2024. As prescribed by the Federal Information Security Modernization Act of 2014 (FISMA), the PBGC Inspector General is required to conduct 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.

Ernst and Young LLP, our independent auditor, completed the Inspector General FISMA metrics that we then submitted to OMB. This year, our independent auditor found PBGC's information security program and practices effective. However, weaknesses were identified in the domains of supply chain risk management, configuration management, data protection and privacy, and security training. PBGC concurred with the report's findings and the six new recommendations to address the identified gaps.

cc: Joshua Kossoy
Tim Hurr
Paul Chalmers
Alice Maroni
David Foley
Karen Morris
Lisa Carter
Latreece Wade
Patricia Kelly
John Hanley
Michael Rae
Walt Luiza

Pension Benefit Guaranty Corporation

Information Security Program and Practices for Fiscal Year 2024

October 31, 2024

Building a better working world

Building a better working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

Tel: +1 703 747 1000
Fax: +1 703 747 0100
ey.com

Report of Independent Auditors on the Pension Benefit Guaranty Corporation's Information Security Program and Practices for Fiscal Year 2024 Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

To: Mr. Nicholas Novak
Inspector General

Re: Pension Benefit Guaranty Corporation (PBGC) Information Security Program and Practices for Fiscal Year 2024

We have conducted a performance audit of the Pension Benefit Guaranty Corporation security program as of July 31, 2024, with the objective of assessing PBGC's effectiveness and consistency with the requirements of the Federal Information Security Modernization Act of 2014 (FISMA) as defined in the FY 2024 Inspector General FISMA Reporting Metrics. PBGC's management is responsible for defining the policies, procedures, and practices supporting the implementation of the PBGC's Information Security Programs in accordance with FISMA reporting metrics.

We conducted this performance audit in accordance with generally accepted *Government Auditing Standards*. 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.

To audit PBGC's effectiveness and consistency with the requirements of FISMA, we applied the Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General FISMA Reporting Metrics. The specific scope and methodology are defined in Appendix A of this report. The nature, timing, and extent of the procedures selected depend on our judgment. This performance audit did not constitute an audit of the financial statements in accordance with auditing standard generally accepted in the United State of America or Government Auditing Standards.

The conclusions and our findings, recommendations, and proposed actions for the improvement of PBGC's effectiveness and consistency with the requirements with FISMA in Section II, were noted as a result of our audit. Management's responses to our reported findings and recommendations are included in Appendix D of this report.

This report is intended solely for the information and use of PBGC, the PBGC Office of Inspector General (OIG), Department of Homeland Security (DHS), Office of Management and Budget (OMB), the appropriate committees of Congress and the Comptroller General and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young LLP

October 31, 2024

Table of Contents

Abbreviations

ATO	Authorization to Operate
BIA	Business Impact Assessments
CISO	Chief Information Security Officer
CCP	Common Control Providers
CMDB	Configuration Management Database
CDM	Continuous Diagnostic and Mitigation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CSRM	Cybersecurity Risk Management Strategy
DHS	Department of Homeland Security
EY	Ernst & Young LLP
EO	Executive Order
CIO	Chief Information Officer
FCEB	Federal Civilian Executive Branch
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FY	Fiscal Year
PBGC	Pension Benefit Guaranty Corporation
IG	Inspector General
IC	Intelligence Community
NIST	National Institute of Standards and Technology
NFR	Notice of Findings and Recommendation
OIG	Office of Inspector General
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PIA	Privacy Impact Assessments
SCRM	Supply Chain Risk Management
SSP	System Security Plans

Section 1
Overview

Section 1: Overview

1.1 Objective

We have conducted a performance audit (also referred to as an audit herein) on the Pension Benefit Guaranty Corporation's (PBGC) (the Corporation) information security program and practices (the Program) to determine whether they were effective and consistent with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), as defined in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[1] (IG FISMA Reporting Metrics) as of July 31, 2024.

1.2 Background

The FISMA was amended on December 18, 2014 (Public Law 113-283). The purpose of FISMA is 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. The amendment included the: (1) 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[2].

FISMA requires Inspector General to perform an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of the information security program and practices of the agency[2]. PBGC's Office of the Inspector General (OIG) engaged us, Ernst & Young LLP, to assess the effectiveness of PBGC's information security controls, including its policies, procedures, and practices on a representative subset of the Corporation's information systems by leveraging work performed as part of the financial statement audit and performing necessary additional testing procedures, as applicable.

FISMA Domains, Metrics and Ratings

The IG FISMA Reporting Metrics were developed in a collaborative effort between (and the consensus opinion of) representatives from OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch (FCEB) Chief Information Security Officers (CISOs) and their staff, and the Intelligence Community (IC). The IG FISMA Reporting Metrics continued using the maturity model approach for all security domains and are

[1] Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics)
[2] *Federal Information Security Management Act of 2014*, Pub. L. No. 113-283, § 2, 128 Stat. 3073, 3075-3078 (2014)

fully aligned with the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity[3] (Cybersecurity Framework) function areas.

The IG FISMA Reporting Metrics are grouped into nine domains and aligned to the five Cybersecurity Framework function areas[4]:

Table 1: Alignment of the Cybersecurity Framework with the IG FISMA Domains

Cybersecurity Framework Function Areas	IG FISMA Domains
Identify	Risk Management
	Supply Chain Risk 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

Reporting Metrics

For the IG FISMA Metrics, the OMB, CIGIE, FCEB CISO, and the IC, continued refining the metrics into (20) Core and (37) Supplemental IG Metrics (Performance Metrics). The 37 supplemental IG Metrics were also further split into previously scored metrics (20), hereinto referred to as FY 2023 Supplemental Metrics, and newly evaluated metrics (17), hereinto referred to as FY 2024 Supplemental Metrics. Core and supplemental metrics were defined as follows:

- Core Metrics – Metrics that are assessed annually and represent a combination of Administration priorities, high impact security processes, and essential functions necessary to determine security program effectiveness.
- Supplemental Metrics – Metrics that are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

[3] NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 (https://www.nist.gov/cyberframework)
[4] See Appendix E for metric domains descriptions.

Maturity Level Scoring

OMB and DHS continued with a calculated scoring model for FY 2024. The maturity level scoring was prepared by OMB and DHS and is divided into calculated scores for core and supplemental metrics. Level 1 (Ad-hoc) is the lowest maturity level and Level 5 (Optimized) is the highest maturity level. The details of the five maturity model levels are:

- Level 1 (Ad-hoc): Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
- Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.
- Level 3 (Consistently Implemented): Policies, procedures, and strategies 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 strategies are collected across the organization and used to assess them and make necessary changes.
- Level 5 (Optimized): Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Within the context of the maturity model, Level 4 (Managed and Measurable) represents an "effective" level of security.

1.3 Audit Scope and Methodology

Scope

In FY 2024, based on OMB and DHS guidance, we performed procedures to assess PBGC's program effectiveness with FISMA. We tested PBGC's information security controls to determine whether PBGC's overall information technology security program and practices were effective as they relate to federal information security requirements.

Methodology

To promote consistency in the annual FISMA evaluations, CIGIE, in coordination with OMB, DHS, and the Federal Chief Information Officers (CIO) and CISO councils developed the FY 2024 IG FISMA reporting metrics evaluation guide, issued April 30, 2024[5]. To assess PBGC's FISMA effectiveness, we leveraged this guide and the PBGC's self-assessed maturity levels to develop our procedures.

For each Core IG FISMA and FY 2024 Supplemental Metrics question, we tested whether PBGC had defined a process to address the requirement through inquiry with management and inspection

[5] Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Evaluator's Guide (https://www.cisa.gov/resources-tools/resources/fy-2024-ig-fisma-metrics-evaluation-guide

of management policies and procedures. For metrics we determined PBGC defined adequately, we performed tests to determine whether they were effectively and consistently implemented. To evaluate the IG FISMA Metrics questions, we performed the following:

- Reviewed applicable Federal laws, regulations, and guidance.

- Gained an understanding of the current security program at PBGC.

- Inquired of PBGC personnel of their self-assessment for each FISMA reporting metric.

- Assessed the status of PBGC's security program against PBGC'S cybersecurity program policies, other standards and guidance issued by PBGC management, and reporting metrics.

- Inspected and analyzed selected artifacts including but not limited to system security plans, evidence to support testing of security controls, Plan of Action & Milestones (POA&Ms) records, security training records, asset compliance reports, system inventory reports and account management documentation.

- Inspected internal assessments performed on behalf of PBGC management that had a similar scope to the FY 2023-2024 IG FISMA metrics. Incorporated the results as part of the FY 2024 IG FISMA metrics.

Based on the results of these tests, we determined whether PBGC met the associated Metric maturity requirements. We then reviewed the results of the Core and Supplemental metrics to determine whether the Corporation was at an overall effective level (Managed and Measurable) for the domain and corresponding function.

Section 2
Conclusions and Enterprise-wide Recommendations

Section 2: Conclusion and Enterprise-wide Recommendations

2.1 Conclusion

Overall, through the evaluation of FISMA metrics, it was determined that PBGC's information security program was "Effective". This determination was made based on the evaluation of PBGC meeting a 'Managed and Measurable' maturity level for the Identify, Protect, Respond, and Recover function areas, and an 'Optimized' maturity level for the Detect function area as required by the FY 2023-2024 Inspector General FISMA Reporting Metrics.

Table 2 below provides the FY 2024 IG FISMA Maturity results and calculated score.

Table 2: 2024 PBGC Maturity Levels and Scores

Function	Domain	Averaged Score for Core Metrics	Averaged Score for FY23 Supplemental Metrics[6]	Averaged Score for FY24 Supplemental Metrics	Effectiveness
Identify	***Risk Management***	4.2	4.66	4	Effective
	Supply Chain Risk Management	4	4	1	
Protect	***Configuration Management***	3.5	4	4	Effective
	Identity & Access Management	4.33	4.5	5	
	Data Protection & Privacy	4.5	3	3.5	
	Security Training	4	4.5	3.5	
Detect	***Information Security Continuous Monitoring***	5	4	5	Effective
Respond	***Incident Response***	4	4	4.66	Effective
Recover	***Contingency Planning***	4	4	4	Effective

Effectiveness in all function areas has been achieved however, some individual metric questions were rated below managed and measurable. It is important for PBGC to continue to focus on remediating its cybersecurity deficiencies to maintain its effective rating. Detailed findings for these domains have been provided, along with others as identified, in Section 3 – Appendix A of this report.

IDENTIFY

[6] We did not perform additional procedures on these specified metrics; we have presented the results as reported in in the report title "The Pension Benefit Guaranty Corporation FY 2023 Federal Information Security Modernization Act (FISMA) Report".

The goal of the Identify function is to develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This area is the foundation that allows an agency to focus and prioritize its efforts with its risk management strategy and business needs. Within this function, there are two domains, Risk Management and Supply Chain Risk Management. Risk Management is at a 'Managed and Measurable' maturity level and Supply Chain Risk Management is at a 'Managed and Measurable' maturity level, therefore our overall assessment of this function was "Effective."

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Identify	Risk Management	Level 4
	Supply Chain Risk Management	Level 4

Risk Management findings

The Risk Management Framework, developed by NIST[7], provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. A risk management framework is the foundation on which an IT security program is developed and implemented by an entity. A risk management framework should include: an assessment of management's long-term plan, documented goals and objectives of the entity, clearly defined roles and responsibilities for security management personnel, and prioritization of IT needs.

For the FY 2024 audit year, there were no identified findings regarding the PBGC Risk Management domain.

Supply Chain Risk Management findings

Supply Chain Risk Management (SCRM) involves activities that pertain to managing cyber supply chain risk exposures, threats, and vulnerabilities throughout the supply chain and developing risk response strategies to the risk presented by the supplier, the supplied products and services or the supply chain.

The following findings were identified within the Corporation's SCRM program:

- PBGC has not fully defined procedures to detect and prevent counterfeit components from entering the organization, to maintain configuration control over organizationally defined system components awaiting repair or being serviced, and to require reporting of counterfeit system components (NFR IT-2024-001).

[7] NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations

PROTECT

The goal of the Protect function is to develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event and incorporates the domains of Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training. The Protect function is at 'Managed and Measurable;' therefore, our overall assessment of this function was "Effective."

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Protect	Configuration Management	Level 4
	Identity and Access Management	Level 4
	Data Protection and Privacy	Level 4
	Security Training	Level 4

Configuration Management findings

Configuration management involves activities that pertain to the operations, administration, maintenance and configuration of networked systems and their security posture. Areas of configuration management include standard baseline configurations, anti-virus management, and patch management.

The following findings were identified within the Corporation's configuration management program:

- PBGC has established policies and procedures for configuration settings/common secure configurations. However, weak security settings have been identified in the Active Directory Certificate Services templates. Additionally, vulnerabilities have also been found in the network segmentation (NFR IT-2024-002).

- Weak network configurations have been identified that could lead to vulnerabilities, potentially allowing attackers to gain unauthorized access to sensitive internal resources (Remediated).

Identity and Access Management (IAM) findings

Federal agencies are required to establish procedures to limit access to physical and logical assets and associated facilities to authorized users, processes, and devices. An appropriate monitoring process should also be implemented to validate that information system access is limited to authorized transactions and functions for each user based on the concept of least privilege.

For the FY 2024 audit year, there were no identified findings regarding the PBGC Identity and Access Management domain.

Data Protection and Privacy findings

Federal agencies have unique access to personally identifiable information (PII) of U.S. citizens. Many of PBGC's systems contain PII. The underlying principle of data privacy and protection controls is to protect the confidentiality of information stored on information systems. To protect this information, Federal regulations such as M-22-09[8] and BOD-18-02[9] have been established requiring agencies to report when this information is stored, how it is protected, and when breaches occur.

The following findings were identified within the Corporation's data protection and privacy program:

- PBGC has defined a privacy program and conducted a Breach Response Team Tabletop exercise that is used to improve collaboration and communication. However, PBGC has not monitored and analyzed quantitative performance measures on the effectiveness of its Data Breach Response Plan (NFR IT-2024-003).

Security Training findings

An effective IT security program cannot be established and maintained without giving enough training to its information system users. Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment and secured physical locations without providing their personnel adequate security training.

The following findings were identified within the Corporations Security Training program:

- PBGC assesses the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. However, employees have not received adequate training to effectively recognize social engineering phone calls. Additionally, the use of weak authentication mechanisms has been found on remote access portals (NFR IT-2024-004).

[8] OMB M-22-09 Federal Zero Trust Strategy (whitehouse.gov)
[9] BOD 18-02: Securing High Value Assets | CISA

- Weak authentication mechanisms on remote access portals have been identified, potentially allowing attackers to compromise accounts and gain unauthorized access to internal network resources.

DETECT

The goal of the Detect function is to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect function enables timely discovery of cybersecurity events. The domain within this function is Information Security Continuous Monitoring (ISCM), which was assessed at 'Optimized', therefore our overall assessment of this function was "Effective".

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Detect	ISCM	Level 5

Information System Continuous Monitoring findings

An ISCM program allows an organization to maintain the security authorization of an information system over time in a dynamic environment of operations with changing threats, vulnerabilities, technologies, and business processes. The implementation of a continuous diagnostic and mitigation (CDM) program results in an approach to fortifying the cybersecurity posture through ongoing updates to system security plans, a periodic security assessment and POA&Ms, which are the three principal documents in a security authorization package.

For the FY 2024 audit year, there were no identified findings regarding the PBGC ISCM domain.

RESPOND

The goal of the Respond function is to develop and implement the appropriate activities to act regarding a detected cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event and is defined by the incident response program. The domain within this function is incident response, which was assessed at 'Managed and Measurable', therefore our overall assessment of this function was 'Effective'.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Respond	Incident Response	Level 4

Incident Response findings

Incident Response involves capturing general threats and incidents that occur in the PBGC systems and physical environment. Incidents are captured by systematically scanning IT network assets for any potential threats, or they are reported by affected persons to the appropriate personnel. For the FY 2024 assessment year, there were no identified findings regarding the PBGC's Incident Response domain.

RECOVER

The goal of the Recover function is to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event or natural disaster. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. The domain that was assessed within this function is Contingency Planning. Due to Contingency Planning being assessed at a maturity level of 'Managed and Measurable', our overall assessment of this function was "Effective".

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2024 IG Assessment
Recover	Contingency planning	Level 4

Contingency Planning findings

Contingency planning refers to a coordinated strategy involving plans, procedures and technical measures that enable the recovery of business operations, information systems and data after a disruption.

Information system contingency planning is unique to each system. Each contingency plan should provide preventive measures, recovery strategies and technical considerations that are in accordance with the system's information confidentiality, integrity and availability requirements and the system impact level.

For the FY 2024 audit year, there were no identified findings regarding the PBGC Contingency Planning domain.

2.2 Recommendations

To strengthen PBGC's enterprise-wide cybersecurity program, based on our reviews across the Corporation, we recommend that PBGC focus on four core areas for an effective program. Additional findings and recommendations are noted in Section III of this report. We recommend PBGC should:

- 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.

- 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.

- Establish robust network segmentation and configure firewalls with default rules to ensure the guest wireless network is effectively isolated from internal resources.

- 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.

- Implement an effective specialized security training program that includes steps to identify and prevent phone-based social engineering for all employees.

- Strengthen its controls around verifying the identity of PBGC personnel prior to temporarily disabling their requirement for MFA for remote access should a user purportedly have a malfunctioning PIV card or other MFA token.

Section 3
Appendices

Section 3: Appendices

3.1 Appendix A: Scope and Methodology

Scope

The Federal Information Security Modernization Act of 2014 (FISMA) directs each agency's Inspector General (IG) to perform, or have an independent external auditor perform, an annual independent evaluation of the agency's information security programs and practices as well as a review of an appropriate subset of agency systems. The objective of Ernst & Young LLP's performance audit was to determine whether PBGC's overall information security program and practices were effective and consistent with FISMA requirements, as defined in the *FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*[10] (IG FISMA Reporting Metrics) as of July 31, 2024.

The FY 2024 IG FISMA reporting metrics were assessed at PBGC and based on the aggregation of their results. In FY 2024, we tested PBGC's information security controls and 9 in scope systems at PBGC.

Methodology

We mapped PBGC's key information security controls to the metrics in the FY 2024 FISMA domains. For each metric question, we tested the design of the control through inquiry with management and inspection of management policies and procedures. For controls we determined PBGC defined adequately, we performed tests to determine whether they were effectively and consistently implemented. Depending on the control, we performed procedures for our 9 in scope systems, random sampling, or inspection of system settings. For specific controls identified for testing we considered suggested controls outlined in the cybersecurity and privacy framework profile of the NIST Special Publication 800-53, Revision 5[11], *Security and Privacy Controls for Information Systems and Organizations* along with the security and privacy control baselines identified in NIST for the Federal Government and tailored this guidance to assist in the control selection process.

To accomplish our objectives, we performed the procedures outlined in our Statement of Work[12] (SOW)'s Planned Scope and Methodology section. This included using federal guidance to conduct:

- Reviewed applicable Federal laws, regulations, and guidance.

- Gained an understanding of the current security program at PBGC.

[10] Office of Management and Budget (OMB), Office of the Federal Chief Information Officer, FY 2023 – 2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics (https://www.cisa.gov/resources-tools/resources/fy23-24-ig-fisma-metrics)

[11] NIST Special Publication 800-53, Revision 5 , Security and Privacy Controls for Information Systems and Organizations (https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)

[12] Contract Number: GS-00F-290CA, Task Order Number 28321323FDX030009

- Inquired of PBGC personnel their self-assessment for each FISMA reporting metric.

- Assessed the status of PBGC' security program against PBGC cybersecurity program policies, other standards and guidance issued by PBGC management, and reporting metrics.

- Inspected and analyzed selected artifacts including but not limited to system security plans, evidence to support testing of security controls, POA&M records, security training records, asset compliance reports, system inventory reports and account management documentation.

- Inspected internal assessments performed on behalf of PBGC management that had a similar scope to the FY 2023-2024 IG FISMA metrics. Incorporated the results as part of the FY 2024 IG FISMA metrics.

Finally, we performed detailed technical security controls testing with the knowledge and consent of the PBGC's Information System staff. For this testing, our team collaborated with the OIG and the PBGC's designated points of contact to agree on the Rules of Engagement that defined the nature, timing, and extent of our technical security work (i.e., diagnostic, or technical security testing outside of our controls work). The NIST Special Publication 800-115[13] guidance was used as the foundation to define the attributes of the technical security testing.

We conducted these procedures in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and 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.

[13] https://csrc.nist.gov/pubs/sp/800/115/final

3.2 Appendix B: List of Findings and Recommendations [14]

Risk Management Findings and Recommendations

- For the FY 2024 audit year, there were no identified findings or recommendations regarding the PBGC Risk Management domain.

Supply Chain Risk Management Findings and Recommendations

- PBGC has not fully defined procedures to detect and prevent counterfeit components from entering the organization, to maintain configuration control over organizationally defined system components awaiting repair or being serviced, and to require reporting of counterfeit system components (NFR IT-2024-001).

- Recommendation: PBGC should 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.

Configuration Management Findings and Recommendations

- PBGC has established policies and procedures for configuration settings/common secure configurations. However, weak security settings have been identified in the Active Directory Certificate Services templates. Additionally, vulnerabilities have also been found in the network segmentation (NFR IT-2024-002).

- Weak network configurations have been identified that could lead to vulnerabilities, potentially allowing attackers to gain unauthorized access to sensitive internal resources (Remediated).

- Recommendation: 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.

- Recommendation: PBGC should establish robust network segmentation and configure firewalls with default rules to ensure the guest wireless network is effectively isolated from internal resources.

[14] Additional conditions identified through security and penetration testing are included separately in the management memo due to data sensitivity.

Identity and Access Management Findings and Recommendations

- For the FY 2024 assessment year, there were no identified findings or recommendations regarding the PBGC's Identity and Access Management domain.

Data Protection and Privacy Findings and Recommendations

- PBGC has defined a privacy program and conducted a Breach Response Team Tabletop exercise that is used to improve collaboration and communication. However, PBGC has not monitored and analyzed quantitative performance measures on the effectiveness of its Data Breach Response Plan (NFR IT-2024-003).

- Recommendation: PBGC should 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.

Security Training Findings and Recommendations

- PBGC assesses the knowledge, skills, and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. However, employees have not received adequate training to effectively recognize social engineering phone calls. Additionally, the use of weak authentication mechanisms has been found on remote access portals (NFR IT-2024-004).

- PBGC has defined their remote connection capabilities within policy. However, weak authentication mechanisms on remote access portals were identified.

- Recommendation: PBGC should implement an effective specialized security training program that includes steps to identify and prevent phone-based social engineering for all employees.

- Recommendation: PBGC should strengthen its controls around verifying the identity of PBGC personnel prior to temporarily disabling their requirement for MFA for remote access should a user purportedly have a malfunctioning PIV card or other MFA token.

Information System Continuous Monitoring Findings and Recommendations

- For the FY 2024 assessment year, there were no identified findings or recommendations regarding the PBGC's Information System Continuous Monitoring domain.

Incident Response Findings and Recommendations

- For the FY 2024 assessment year, there were no identified findings or recommendations regarding the PBGC's Incident Response domain.

Contingency Planning Findings and Recommendations

- For the FY 2024 assessment year, there were no identified findings or recommendations regarding the PBGC's Contingency Planning domain.

3.3 Appendix C: Federal Requirements and Guidance

The principal criteria used for this performance audit included:

- DHS Binding Operational Directive 18-02, Securing High Value Assets, (May 07, 2018)
- DHS Binding Operational Directive 19-02, Vulnerability Remediation Requirements for Internet-Accessible Systems, (April 29, 2019)
- DHS Binding Operational Directive 22-01, Reducing Significant Risk of Known Exploited Vulnerabilities, (November 03, 2021)
- Executive Order on Improving the Nation's Cybersecurity (EO 14028) (May 12, 2021)
- IG FISMA Metrics Evaluation Guide (2024 Publication)
- Federal Information Security Modernization Act of 2014 (December 2014)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems (February 2004).
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006).
- PBGC Information Security Risk Management Framework (RMF) Process (April 2024)
- PBGC Infrastructure Configuration Management Plan (ICMP) (May 2023)
- PBGC Enterprise Continuous Monitoring (ECM) Strategy and Plan (February 2024)
- PBGC Office of Information Technology Data Loss Prevention Standard Operating Procedure (June 2023)
- PBGC Security and Privacy Literacy Training Procedures (January 2024)
- PBGC Information Security Policy Directive IM 05-02 (May 8, 2023)
- PBGC Incident Management Operational Procedure (May 2023)
- PBGC Enterprise Continuity of Operations Plan (COOP) (December, 2023)
- NIST SP 800-34 Contingency Planning Guide for Federal Information Systems (May 2010).
- NIST SP 800-37, revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (December 2018).
- NIST SP 800-53, revision 5, Security and Privacy Controls for Federal Information Systems and Organizations (September 2020).

- NIST SP 800-61, Computer Security Incident Handling Guide (August 2012).
- NIST IR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM) (October 2020)
- NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (September 2011).
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007).
- OMB M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program (December 10, 2018)
- OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019)
- OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control
- OMB M-21-30, Protecting Critical Software Through Enhanced Security Measures (August 10, 2021)
- OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents (August 27, 2021)
- OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (October 08, 2021)
- OMB M-22-05, Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (December 6, 2021)
- OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022)
- OMB M-24-04 Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements (December 4, 2023)

3.4 Appendix D: Management's Response to findings and recommendations

PBGC Pension Benefit Guaranty Corporation

445 12th Street SW
Washington, DC 20024-2101
202-229-4000
PBGC.gov

October 25, 2024

MEMORANDUM

To: Nicholas J. Novak
Inspector General

From: Joshua Kossoy, ITIOD Director JOSHUA KOSSOY Digitally signed by JOSHUA KOSSOY Date: 2024.10.25 12:59:24 -04'00'

Tim Hurr, Chief Information Security Officer (CISO) Digitally signed by TIEN HURR Date: 2024.10.25 13:13:47 -04'00'

Paul Chalmers, Deputy General Counsel CHARLES CHALMERS Digitally signed by CHARLES CHALMERS Date: 2024.10.25 14:03:01 -04'00'

Subject: Response to OIG's Draft Fiscal Year 2024 FISMA Report

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, received October 11, 2024, relating to Pension Benefit Guaranty Corporation's (PBGC) Implementation of the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2024. Your office's work on this is sincerely appreciated.

PBGC management concurs with the report's 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 PBGC.

Attachment

cc:
Ann Orr
Alice Maroni
David Foley
Karen Morris
Lisa Carter
Latreece Wade
Robert Scherer
Patricia Kelly
John Hanley
Michael Rae
Walt Luiza

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

1. **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. (OIG Control Number 2025-02-01-OIT)**

   PBGC Response: PBGC concurs with this recommendation. OIT is developing an enterprise-wide approach to prevent counterfeit components from entering PBGC's supply chain, including performance measures to gauge the effectiveness of the policies and procedures.

   Scheduled Completion Date: June 30, 2025

2. **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. (OIG Control Number 2025-02-02-OIT)**

   PBGC Response: PBGC concurs with this recommendation. OIT will harden Active Directory certificate template settings and audit existing templates. This will include an assessment of privileged access to the templates to prevent unauthorized changes.

   Scheduled Completion Date: June 30, 2025

3. **PBGC should establish robust network segmentation and configure firewalls with default rules to ensure the guest wireless network is effectively isolated from internal resources. (OIG Control Number 2025-02-03-OIT)**

   PBGC Response: PBGC concurs with this recommendation. OIT has remediated the firewall configurations. However, OIT will implement controls to ensure continued effective isolation of the guest wireless network from internal resources.

   Scheduled Completion Date: June 30, 2025

4. **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. (OIG Control Number 2025-02-04-OGC)**

   PBGC Response: PBGC concurs with this recommendation. PBGC has already begun collecting metrics to support this analysis. We will use the newly collected metrics in support of the annual Breach Response Plan update.

   Scheduled Completion Date: December 31, 2025

5. **PBGC should implement an effective specialized security training program that includes steps to identify and prevent phone-based social engineering for all employees. (OIG Control Number 2025-02-05-OIT)**

   PBGC Response: PBGC concurs with this recommendation. OIT has started developing a specialized security training program for all employees that includes steps to identify and prevent phone-based social engineering.

   Scheduled Completion Date: June 30, 2025

6. **PBGC should strengthen its controls around verifying the identity of PBGC personnel prior to temporarily disabling their requirement for MFA for remote access should a user purportedly have a malfunctioning PIV card or other MFA token. (OIG Control Number 2025-02-06-OIT)**

   PBGC Response: PBGC concurs with this recommendation. OIT is in the process of strengthening controls around verifying the identity of PBGC personnel prior to temporarily disabling their requirements for multifactor authentication (MFA).

   Scheduled Completion Date: June 30, 2025