OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

Pension Benefit Guaranty Corporation's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2022

Report No. AUD-2023-06
January 9, 2023

January 9, 2023

MEMORANDUM

TO: Gordon Hartogensis
Director

FROM: Nicholas J. Novak
Inspector General *Nicholas J. Novak*

SUBJECT: PBGC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2022 (AUD-2023-06)

I am pleased to transmit the Pension Benefit Guaranty Corporation's Federal Information Security Modernization Act of 2014 (FISMA) audit report detailing the results of our review of the PBGC information security program.

As prescribed by FISMA, the PBGC Inspector General is required to conduct annual evaluations of PBGC's security programs and practices, and to report to the Office of Management and Budget (OMB) the results of this evaluation. Ernst and Young LLP, on behalf of the OIG, completed the OMB-required responses that we then submitted to OMB. This year, Ernst and Young LLP issued four new FISMA-related recommendations. PBGC agreed with the four new recommendations in this report.

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

cc: Robert Scherer
Kristin Chapman
Patricia Kelly
Karen Morris
John Hanley
Alice Maroni
Ann Orr
Dave Foley
Frank Pace

Pension Benefit Guaranty Corporation

FY 2022 Federal Information Security Modernization Act (FISMA) Report

January 06, 2023

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 Pension Benefit Guaranty Corporation's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022 Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

Mr. Nicholas Novak

Inspector General

We have conducted a performance audit of the implementation of the Federal Information Security Modernization Act of 2014 (FISMA) by Pension Benefit Guaranty Corporation (PBGC) as of September 30, 2022, as defined in the FY 2022 Inspector General 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.

This performance audit did not constitute an audit of financial statements in accordance with auditing standards generally accepted in the United States of America or *Government Auditing Standards*. The specific scope and methodology are defined in Appendix A of this report.

Findings, Conclusions and Recommendations

The conclusions in Section II and our findings and recommendations, as well as proposed alternatives for the improvement of PBGC's implementation of the FISMA in Section III, were noted as a result of our audit. Management's responses to our findings and recommendations are captured in Appendix C of this report.

This report is intended solely for the information and use of PBGC, the PBGC Office of Inspector General (OIG), the Department of Homeland Security (DHS), the 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

January 06, 2023

Office of Inspector General

Report in Brief – January 06, 2023

Why we did this audit

The Federal Information Security Modernization Act of 2014 (FISMA) requires Inspectors General to perform an annual independent evaluation of their agency's information security programs and practices to determine the effectiveness of those programs and practices. PBGC OIG engaged Ernst & Young LLP (EY) to conduct this audit.

EY conducted a performance audit of PBGC's implementation of the FISMA as of September 30, 2022, based upon the FISMA reporting metrics for the Inspectors General.

Our objective was to determine whether PBGC's overall information technology security program and practices were effective as they relate to federal information security requirements.

How we did this audit

We reviewed applicable federal laws, regulations and guidance; gained an understanding of the current security program at PBGC; assessed the status of PBGC's security program against PBGC-assessed maturity levels, selected information security program policies, other standards and guidance issued by PBGC management, and prescribed performance measures; inquired of personnel to gain an understanding of the FISMA reporting metric areas; and inspected selected artifacts.

Review of the Pension Benefit Guaranty Corporation's implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2022

What we found

Overall, through the evaluation of FISMA metrics, it was determined that PBGC's information security program was "Effective." This determination was made based on (1) the evaluation of PBGC meeting a 'Managed and Measurable' maturity level for the Identify, Protect, Respond, and Recover function areas and 'Optimized' maturity level for the Detect function area as required by the FY 2022 Inspector General FISMA Reporting Metrics. Specific recommendations were also provided to PBGC management for continued improvement.

Progress continues to be made to sustain cybersecurity maturity across all FISMA domains. We noted an increased maturation of the Supply Chain Risk Management and Information Security Continuous Monitoring domains. While PBGC can be considered effective, we identified opportunities where PBGC can strengthen its program within Configuration Management and Identity and Access Management.

What we recommend

PBGC has an effective security program; 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.

PBGC should work to integrate its information security architecture with its systems development lifecycle. Additionally, PBGC should continue to implement improvement throughout segregation of duties and authentication to minimize risk throughout PBGC. Lastly, PBGC should continue to improve in the areas in Configuration Management, and Identity and Access Management domains.

Table of Contents

Section 1
Background

1.1 Introduction

Ernst & Young LLP (EY) conducted a performance audit of Pension Benefit Guaranty Corporation (PBGC) regarding its compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2022, based upon the questions outlined in the FISMA reporting metrics for the Inspectors General (IGs).

1.2 Background

On December 17, 2002, the President signed the Federal Information Security Management Act into law as part of the E-Government Act of 2002 (Public Law 107-347, Title III). 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. FISMA was amended on December 18, 2014 (Public Law 113-283). The amendments included the (1) re-establishment 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 through assessing the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of such information or information systems.

To comply with the FISMA, the OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), Federal Civilian Executive Branch Chief Information Security Officers and their staff, and the intelligence community (IC) developed the FY 2022 IG FISMA reporting metrics, issued April 13, 2022. FISMA requires IGs independently evaluate the information security program and practices of the agency annually to determine the effectiveness of the information security program and practices of the agency. The FY 2022 evaluation was completed by EY, under contract to the PBGC Office of Inspector General as a performance audit in accordance with *Government Auditing Standards* of the Government Accountability Office (GAO).

Cybersecurity Framework

The cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks. The FY 2022 IG metrics mark a continuation of the work that began in FY 2016 when the IG metrics were aligned to the five function areas in the *National Institute of Standards and Technology (NIST) Framework for Improving Critical infrastructure Cybersecurity*: Identify, Protect, Detect, Respond, and Recover.

For FY 2022, updates were made to the IG FISMA metrics to align with Executive Order (EO) 14028 of May 12, 2021, *Improving the Nation's Cybersecurity*, as well as OMB guidance M-22-09, M-21-31, M-22-05 and M-22-01 to agencies in furtherance of the modernization of federal cybersecurity. As a result, 20 core IG metrics were selected for evaluation as to the effectiveness of the organization.

The FY 2022 IG FISMA reporting metrics are grouped into nine domains and organized around the five cybersecurity framework function areas:

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 (ISCM)
Respond	Incident Response
Recover	Contingency Planning

Reporting Metrics

For the FY 2022 IG FISMA metrics, a series of metrics (or questions) was developed for each IG FISMA domain to assess the effectiveness of an agency's cybersecurity framework (Identify, Protect, Detect, Respond and Recover).

Maturity Level Scoring

The maturity-level scoring was prepared by OMB and DHS. 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, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

Per OMB and DHS, within the context of the maturity model, Level 4 (Managed and Measurable) represents an "effective" level of security. However, DHS does allow OIGs to

deviate from the standard for determining the “effective” level of security. OIGs have the discretion to determine the overall effectiveness rating and the rating for each Cybersecurity Framework function (Identify, Protect, Detect, Respond, and Recover) at the maturity level of their choosing, which allows for agency-specific considerations to be factored in.

Section 2
Conclusion and Enterprise-wide Recommendations

2.1 Conclusions

Conclusion

Our specific conclusions related to PBGC's cybersecurity program for each FISMA domain are based on the FISMA reporting metrics loaded within CyberScope.

Based on the results of our performance audit of the 20 core metrics, we determined that PBGC's cybersecurity program was "effective," as it met the criteria required to be assessed at a 'Managed and Measurable' maturity level for four selected function areas: Identify, Protect, Respond and Recover, and 'Optimized' for the Detect function area.

Progress for FY 2022

As with the prior year, this performance audit was conducted with the constraints of COVID-19. Thus, the audit procedures followed the FY 2020 and FY 2021 revised approach to allow for a virtual approach. In addition, new risk areas arose that resulted in the shifting of cybersecurity postures due to the increase of telework for the corporation.

Table 2 below provides the FY 2022 IG FISMA maturity results. In FY 2022, improvements in the overall posture were evident with the increase in maturity levels for individual metrics. Areas where PBGC's security program needed improvement are captured by our specific findings and recommendations in Section 2.2.

Table 2: 2022 PBGC Maturity Levels

Function	Domain	OIG Assessed Maturity	FY 2022 IG Assessment vs FY 2021 IG Assessment
Identify	Risk Management	Managed and Measurable (Level 4)	No change
	Supply Chain Risk Management	Managed and Measurable (Level 4)	Increased two (2) levels
Protect	Configuration Management	Managed and Measurable (Level 4)	No change
	Identity & Access Management	Managed and Measurable (Level 4)	No change
	Data Protection & Privacy	Managed and Measurable (Level 4)	No change

	Security Training	Managed and Measurable (Level 4)	No change
Detect	Information Security Continuous Monitoring	Optimized (Level 5)	Increased one (1) level
Respond	Incident Response	Managed and Measurable (Level 4)	No change
Recover	Contingency Planning	Managed and Measurable (Level 4)	No change

Specifically within the Supply Chain Risk Management domain, we noted that PBGC's cybersecurity program improvements supported an increased rating due to the following:

- Improvements surrounding digital threat monitoring
- Implementation of a digital threat monitoring tool that produces near real-time threat actor, malware and vulnerability tracking
- Improvements in managing cyber risk and vulnerabilities
- Implementation of supplier risk evaluations

Specifically within the Information Security Continuous Monitoring domain, we noted that PBGC's cybersecurity program improvements supported an increased rating due to the following:

- Improvements surrounding the integration of PBGC's ISCM policies and strategy with its enterprise and supply chain risk management, configuration management, incident response, and business continuity programs
- Improvements in tracking and monitoring cost savings of PBGC's continuous monitoring program

2.2 Cybersecurity Framework Domain Findings and Recommendations

This section consolidates findings identified during our audit of the PBGC security program and includes recommendations that should support PBGC in achieving a higher maturity state. We identified findings in PBGC's security program and consolidated them into each of the nine domains below.

2.2.1 Identify

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, for evaluation within the IG metrics. Both Risk Management and Supply Chain Risk Management were determined to be at the "Managed and Measurable' maturity level; therefore, our overall assessment of this function was "effective."

Risk Management

The risk management framework, developed by NIST, provides a disciplined and structured process that integrates information security and risk management activities into the system development lifecycle. 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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Identify	Risk Management	Managed and Measurable	No change

PBGC's Risk Management function has the following in place:

- PBGC maintains an inventory of its information systems and subjects these information systems to the monitoring processes defined within the organization's ISCM strategy.
- PBGC uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets and verifies that the hardware assets connected to the network are covered by an organization-wide hardware asset management capability and are subject to the monitoring processes defined within the organization's ISCM strategy.
- PBGC uses its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses and verifies that software assets on the network (and their associated licenses) are covered by an organization-wide software asset management (or mobile device management) capability and are subject to the monitoring processes defined within the organization's ISCM strategy. PBGC leverages Microsoft Intune to monitor data on mobile devices; therefore, the agency enforces the capability to prevent the execution of unauthorized software.
- PBGC employs various diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of cybersecurity risks across the organization, presenting qualitative and quantitative metrics that provide indicators of cybersecurity risk. Cybersecurity risks are integrated into enterprise-level dashboards and reporting frameworks.

- PBGC uses automation to perform scenario analysis and model potential responses, including modeling the potential impact of a threat exploiting a vulnerability and the resulting impact to organizational systems and data. In addition, the organization integrates cybersecurity risk management information into ERM reporting tools, such as a governance, risk management and compliance tools, as appropriate.

Risk Management Finding and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC Risk Management domain.

Supply Chain Risk Management

Supply Chain Risk Management 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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Identify	Supply Chain Risk Management	Managed and Measurable	Increased two (2) levels

PBGC's Supply Chain Risk Management (SCRM) function has the following in place:

- PBGC confirms that products, system components, systems and services of external providers are consistent with the organization's cybersecurity and supply chain requirements.

Supply Chain Risk Management Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC Supply Chain Risk Management domain.

2.2.2 Protect

The goal of the Protect function is to develop and implement the appropriate safeguards to facilitate delivery of critical infrastructure services. Protect 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. Our overall assessment of this function was "effective."

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Protect	Configuration Management	Managed and Measurable	No change
	Identity and Access Management	Managed and Measurable	No change
	Data Protection and Privacy	Managed and Measurable	No change
	Security Training	Managed and Measurable	No change

Configuration Management

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, antivirus management and patch management.

PBGC's configuration management function has the following in place:

- PBGC employs automation to help maintain an up-to-date, complete, accurate, readily available view of the security configurations for all information system components connected to the organization's network.

Configuration Management Finding and Recommendations

For the FY 2022 assessment year, the following finding was identified with PBGC's configuration management domain:

- Inadequate security protocol configurations were noted on selected servers that allowed for escalation of user account privileges.

PBGC should consider the following recommendations to continue to improve their security posture:

- Disable less secure security authentication protocols on applicable servers and, where not possible, implement mitigating solutions (2023-06-01)

PBGC Response

PBGC concurs with the finding and recommendations. PBGC has implemented some recommended steps such as disabling Encrypting File System (EFS) on all domain controllers via Government Publishing Office (GPO). In addition, the team is currently implementing additional remediations to mitigate the identified issue.

Identity and Access Management

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.

PBGC's Identity and Access Management function has the following in place:

- PBGC has consistently implemented authentication mechanisms for non-privileged users of the organization's facilities and networks, including for remote access, in accordance with Federal targets. Further, PBGC ensures all non-privileged users use strong authentication mechanisms to authenticate.
- PBGC has planned for the use of authentication mechanisms for privileged users of the organization's facilities, systems and networks, including the completion of digital identity risk assessments. Further, PBGC has consistently implemented strong authentication mechanisms for privileged users of the organization's facilities and networks, including for remote access, in accordance with federal targets.

Identity and Access Management Findings and Recommendations

The following findings were identified with PBGC's identity and access management program:

- Inadequate user authentication settings were noted on selected servers, such as passwords between lower and higher privileges were not differentiated, inadequate sessions alignment, and passwords not sufficiently masked within administrator accounts.

PBGC should consider the following recommendations to continue to improve its security posture:

- Users with multiple accounts of different privilege levels should be educated about the risks of reusing passwords for privileged accounts. Procedures for issuing privileged accounts should include language requiring the account be configured with a unique password, at all times. Additionally, consider auditing privileged account passwords for password reuse on a regular basis. (2023-06-02)
- Create separate accounts with the least privileges required to perform administrative tasks on hosts that are not domain controllers. (2023-06-03)
- PBGC should evaluate the privileges associated with accounts configured to run critical services following the least privilege model so that service accounts are assigned the minimum level of privileges needed to perform their individual function. Additionally, PBGC should assign strong passwords to service accounts. (2023-06-04)

PBGC concurs with the finding and recommendations. PBGC will take remediation steps to include developing notifications and guidance for the users identified in the report, updating the PBGC Rules of Behavior to state that a user's privileged account password should be different than their regular user account password, and developing additional processes to identify instances of this issue as they arise. PBGC will perform an assessment against the domain admin accounts and service accounts and follow Microsoft's best practice guidance under Enhanced Security Administrative Environment. PBGC will evaluate the privileges associated with identified accounts configured to run critical services following the least privilege model so that service accounts are assigned the minimum level of privileges needed to perform their individual function.

Data Protection and Privacy

Federal agencies have unique access to personally identifiable information (PII) of US citizens. 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 have been established requiring agencies to report when this information is stored, how it is protected and when breaches occur.

PBGC's Data Protection and Privacy function has the following in place:

- PBGC's policies and procedures have been consistently implemented for the specified areas, including (i) use of Federal Information Processing Standards (FIPS)-validated encryption of PII and other agency sensitive data, as appropriate, both at rest and in transit; (ii) prevention and detection of untrusted removable media; and (iii) destruction or reuse of media containing PII or other sensitive agency data. Further, PBGC subjects the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle to the monitoring processes defined within the organization's ISCM strategy.
- PBGC analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. The organization also conducts exfiltration exercises to measure the effectiveness of its data exfiltration and enhanced network defenses.

Data Protection and Privacy Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC's Data Protection and Privacy domain.

Security Training

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.

PBGC's security training program has the following in place:

- PBGC assesses the knowledge, skills and abilities of its workforce to tailor its awareness and specialized training and has identified its skill gaps. Further, the organization

periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's awareness and training strategy/plans. Further, PBGC has addressed its identified knowledge, skills and abilities gaps through training or talent acquisition.

Security Training Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC Security Training domain.

2.2.3 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). Our overall assessment of this function was "Effective."

Information Security Continuous Monitoring

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 monitoring program results in ongoing updates to system security plans, a periodic security assessment and POA&Ms (plans of actions and milestones), which are three principal documents in a security authorization package.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Detect	ISCM	Optimized	Increased one (1) level

PBGC's ISCM function has the following in place:

- PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates, as appropriate. The organization verifies that data supporting metrics are obtained accurately, consistently and in a reproducible format.
- PBGC developed and consistently implements its system-level continuous monitoring strategies and related processes. Further, PBGC utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.

ISCM Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC ISCM domain.

2.3.4 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. Our overall assessment of this function was "effective."

Incident Response

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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Respond	Incident Response	Managed and Measurable	No change

PBGC's Incident Response function has the following in place:

- PBGC uses its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis and prioritization. Further, PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis policies and procedures.
- PBGC has defined and consistently implements its incident handling policies, procedures, containment strategies and incident eradication processes. Further, PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident handling policies and procedures. PBGC verifies that data-supporting metrics are obtained accurately, consistently, and in a reproducible format.

Incident Response Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC Incident Response domain.

2.2.5 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. 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. Our overall assessment of this function was "effective."

Contingency Planning

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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2022 IG Assessment	Change from FY 2021 IG Assessment
Recover	Contingency Planning	Managed and Measurable	No change

PBGC's Contingency Planning function has the following in place:

- PBGC consistently implements its defined information system contingency planning policies, procedures and strategies. Further, PBGC integrates the results of organizational and system-level business impact analysis (BIA) with enterprise risk management processes, for consistently evaluating, recording and monitoring the criticality and sensitivity of enterprise assets.
- PBGC has defined policies, procedures and processes for information system contingency plan testing and consistently implements information system contingency plan testing and exercises. Further, PBGC employs automated mechanisms to effectively test system contingency plans.

Contingency Planning Findings and Recommendations

For the FY 2022 audit year, there were no identified findings regarding the PBGC Contingency Planning domain.

Section 3
Appendices

Appendix A
Audit Scope and Methodology

Scope

In conjunction with work being undertaken for the PBGC financial statement audit, we performed procedures to assess, based on OMB and DHS guidance, PBGC's compliance with FISMA. To assess PBGC's FISMA compliance, we leveraged the FISMA reporting metrics for the inspector general. We also developed a Notice of Findings and Recommendation (NFR) for each finding identified during testing and provided the NFRs to PBGC after the OIG's review and concurrence.

Methodology

To accomplish our objective, we:

- Reviewed applicable federal laws, regulations and guidance
- Gained an understanding of the current security program at PBGC
- Inquired of PBGC personnel their self-assessment for each FISMA reporting metric
- Assessed the status of PBGC's 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 results from GAO and OIG audits and reports that had a similar scope to the FY 2022 IG FISMA metrics, incorporated the results as part of the FY 2022 IG FISMA metrics, and identified related findings and recommendations from prior year assessments within this report that continue to impact the subject matter
- Inspected artifacts provided by PBGC related to the status of prior year audit issues to determine the extent to which testing of corrective actions was applicable to our current audit objectives

We conducted these procedures in accordance with *Generally Accepted Government Auditing Standards* (GAGAS). 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.

Appendix B
Federal Requirements and Guidance

The principles criteria used for this audit include the following:

- DHS Binding Operational Directive 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems* (April 29, 2019)
- Federal Information Security Modernization Act of 2014 (December 2014)
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004); FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006); PBGC Cybersecurity Program, Standard for Encryption of Computing Devices and Information (December 14, 2016); and PBGC Office of Information Security, *High-Value Asset Program Policy* (March 2018)
- PBGC Information Security Risk Management Framework (RMF) Process (April 2022)
- PBGC Infrastructure Configuration Management Plan (ICMP) (May 2022)
- PBGC Enterprise Continuous Monitoring (ECM) Strategy and Plan (January 2022)
- PBGC Office of Information Technology Data Loss Prevention Standard Operating Procedure (April 2022)
- PBGC Cybersecurity Awareness Training Program Procedure (April 2021)
- PBGC Information Security Policy Directive IM 05-02 (April 22, 2020)
- PBGC Security Incident Management Operational Procedure (May 10, 2021)
- PBGC Enterprise Continuity of Operations Plan (COOP) (June 30, 2021)
- Homeland Security Presidential Directive 12 (HSPD 12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004)
- NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems* (May 2010)
- NIST SP 800-37, revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (June 2014)
- 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)
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007)
- OMB M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (December 6, 2021)
- US-CERT Federal Incident Notification Guideline

Appendix C
PBGC Management Response

PBGC Pension Benefit Guaranty Corporation

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

December 14, 2022

MEMORANDUM

To: Nicholas J. Novak
Inspector General

From: Joshua Kossoy
ITIOD Director

JOSHUA KOSSOY
Digitally signed by JOSHUA KOSSOY
Date: 2022.12.13 09:46:55 -05'00'

Subject: Response to OIG's Draft Fiscal Year 2022 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 2022. 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 Frank Pace should you have any questions.

cc:

Kristin Chapman	Patricia Kelly
Ann Orr	Russell Dempsey
David Foley	Alice Maroni
Karen Morris	Robert Scherer
Frank Pace	Theodore J. Winter

OIG Recommendation No. 2023-06-01: Disable less secure security authentication protocols on applicable servers and where not possible, implement mitigating solutions.

PBGC Response: PBGC concurs with this recommendation. PBGC has implemented some recommended steps such as disabling Encrypting File System (EFS) on all Domain Controllers via Group Policy Object (GPO). In addition, the PBGC is implementing additional steps to remediate the identified issue.

Target Completion Date: 6/30/2023

OIG Recommendation No. 2023-06-02: Users with multiple accounts of different privilege levels should be educated about the risks of reusing passwords for privileged accounts. Procedures for issuing privileged accounts should include language requiring the account be configured with a unique password, at all times. Additionally, consider auditing privileged account passwords for password reuse on a regular basis.

PBGC Response: PBGC concurs with this recommendation. PBGC will take remediation steps to include developing notifications and guidance for the users identified in the report, updating the PBGC Rules of Behavior to state that a user's privileged account password should be different than their regular user account password, and developing additional processes to identify instances of this issue as they arise.

Target Completion Date: 8/31/2023

OIG Recommendation No. 2023-06-03: Create separate accounts with the least privileges required to perform administrative tasks on hosts that are not domain controllers

PBGC Response: PBGC concurs with this recommendation. PBGC will perform an assessment against the domain admin accounts and service accounts and follow Microsoft's best practice guidance under Enhanced Security Administrative Environment.

Target Completion Date: 6/30/2023

OIG Recommendation No. 2023-06-04: PBGC should evaluate the privileges associated with accounts configured to run critical services following the least privilege model so that service accounts are assigned the minimum level of privileges needed to perform their individual function. Additionally, PBGC should assign strong passwords to service accounts.

PBGC Response: PBGC concurs with this recommendation. PBGC will evaluate the privileges associated with identified accounts configured to run critical services following the least privilege model so that service accounts are assigned the minimum level of privileges needed to

perform their individual function. Additionally, PBGC will ensure that associated passwords are of the appropriate length and complexity to adhere to PBGC policy.

Target Completion Date: 6/30/2023

Appendix D
Additional Details Related to IT NFRs

Appendix D provided the cause, criteria, effect and recommendation number associated with IT NFRs.

IT NFR Number	Cause	Condition	Criteria	Effect	Recommendation
NFR IT-2022-001-FISMA-VAPT	Inadequate user authentication settings were noted on selected servers, such as passwords between lower and higher privileges were not differentiated, vulnerable host authentication security protocols, inadequate sessions alignment, and passwords not sufficiently masked within administrator accounts.	• Several domain users' lower-privileged accounts shared the same password as their corresponding higher-privileged accounts. • A vulnerability was exploited using an attack vector by triggering an authentication attempt from a domain controller. • Three domain administrator accounts with sessions on 18 systems were not domain controllers. • EY was able to recover the cleartext passwords for	Center for Internet Security (CIS) security controls	Increased likelihood that allows an attacker to gain unauthorized access to multiple and possibly critical resources, such as privileged access to the network. Access to the network can be circumvented by not resolving known vulnerabilities.	We recommend PBGC complete the following to assist with the remediation of this finding: • Disable less secure security authentication protocols on applicable servers and, where not possible, implement mitigating solutions (2023-06-01) • Educate users with multiple accounts of different privilege levels about the risks of reusing passwords • least privilege model so that service accounts are assigned the minimum level of privileges needed to perform their individual function and assign strong passwords to service accounts (2023-06-02) • Create separate accounts with the least privileges required to perform administrative tasks on hosts that are not domain controllers (2023-06-03) • Evaluate the privileges associated with accounts

		several domain/ enterprise administrator accounts.			configured to run critical services following the least privilege model so that service accounts are assigned the minimum level of privileges needed to perform their individual function and assign strong passwords to service accounts (2023-06-04)

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2212-4152056
ED None

ey.com