PBGC
Protecting America's Pensions

OFFICE OF INSPECTOR GENERAL
AUDIT REPORT

Pension Benefit Guaranty Corporation's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2021

Report No. AUD-2022-7
February 3, 2022

February 3, 2022

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 2021 (AUD-2022-7)

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 the PBGC security programs and practices, and to report to the Office of Management and Budget 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 three new FISMA-related recommendations. PBGC agreed with the three 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
Russ Dempsey
Alice Maroni
Ann Orr
Dave Foley
Frank Pace

Pension Benefit Guaranty Corporation

Federal Information Security Modernization Act Report

January 31, 2022

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 2021 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, 2021, as defined in the FY 2021 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), 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.

January 31, 2022

Report in Brief

Date: January 31, 2022

Office of Inspector General
Pension Benefit Guaranty Corporation

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, 2021, based upon the FISMA reporting metrics defined by 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 2021

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 Identify, Detect, Protect, Respond, and Recover functional areas (2) the upgrade of Identify, Protect, and Recover functional areas from Consistently Implemented to Managed and Measurable ratings. 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 Risk Management, Identity and Access Management, Data Protection and Privacy, and Contingency Planning domains. While PBGC can be considered effective, we identified opportunities where PBGC can strengthen its program within Identity and Access Management.

What we recommend

PBGC has an effective security program, however there were individual metric question that were rated below managed and measurable. While we did not identify those areas, in aggregate, impacted our effectiveness conclusion improvement could be made. It is important for PBGC to continue to focus on remediating their cybersecurity deficiencies to maintain their effective rating.

PBGC should work to integrate their information security architecture with its systems development lifecycle. PBGC should implement updated policies and procedures surrounding the sourcing of hardware and software in accordance with new Supply Chain Risk Management (SCRM) standards. Specifically, PBGC should work towards an organization-wide SCRM strategy and implement policies, procedures, and processes of managing supply chain risks. Additionally, PBGC should continue to implement improvement throughout segregation of duties to minimize risk throughout PBGC. Lastly, PBGC should continue to push in the areas in Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, and Data Protection and Privacy domains.

Table of Contents

Section 1
Background

Section 1: Background

1.1 Introduction

Ernst & Young LLP (EY) conducted a performance audit of the Pension Benefit Guaranty Corporation's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2021, based upon the questions outlined in the FISMA reporting metrics for the Inspectors General (IG).

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, OMB, DHS and the Council of the Inspectors General on Integrity and Efficiency (CIGIE) developed the FY 2021 IG FISMA reporting metrics, issued May 12, 2021, in consultation with the Federal Chief Information Officers Council. These metrics leverage the *National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework)* and are aligned with the five function areas: Identify, Protect, Detect, Respond and Recover. FISMA requires Inspectors 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. The FY 2021 evaluation was completed by Ernst & Young LLP, 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 2021 metrics also mark a continuation of the work that OMB, DHS and CIGIE undertook in FY 2016 to transition the IG assessments to a maturity model approach. This is the third year that all FISMA security domains were assessed using a maturity model.

For FY 2021, updates were made to the IG FISMA questions, as reported in the FY 2021 IG FISMA Reporting Metrics Version 1.1, dated May 12, 2021, which include:

- An additional focus on the Federal Acquisition Supply Chain Security Act of 2018, agencies are required to assess, avoid, mitigate, accept, or transfer supply chain risks. The FY 2021 IG FISMA Reporting Metrics include a new domain on Supply Chain Risk Management (SCRM) within the Identify function. This new domain focuses on the maturity of agency SCRM strategies, policies and procedures, plans, and processes to ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain risk management requirements. The new domain references SCRM criteria in NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations. To provide agencies with sufficient time to fully implement NIST 800-53, Rev 5., in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating.

- Also, within the Identify function, specific metric questions have been reorganized and reworded to focus on the degree to which cyber risk management processes are integrated with enterprise risk management (ERM) processes. As an example, IGs are directed to evaluate how cybersecurity risk registers are used to communicate information at the information system, mission/business process, and organizational levels. These changes are consistent with NIST Interagency Report 8286, "Integrating Cybersecurity and Enterprise Risk Management (ERM)," which provides guidance to help organizations improve the cybersecurity risk information they provide as inputs to their enterprise ERM programs.

- Lastly, OMB has issued guidance on improving vulnerability identification, management, and remediation. Specifically, Memorandum M-20-32, Improving Vulnerability Identification, Management, and Remediation, September 2, 2020, provides guidance to federal agencies on collaborating with members of the public to find and report vulnerabilities on federal information systems. In addition, DHS Binding Operational Directive 20-01, Develop and Publish a Vulnerability Disclosure Policy, September 2, 2020, provides guidance on the development and publishing of an agency's vulnerability disclosure policy and supporting handling procedures. The IG FISMA Reporting Metrics include a new question (#24) to measure the extent to which agencies utilize a vulnerability disclosure policy (VDP) as part of their vulnerability management program for internet-accessible federal systems.

The FY 2021 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 2021 IG FISMA Metrics, a series of metrics (or questions) was developed for each IG FISMA domain (Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response and Contingency Planning) 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:

1. Level 1 (Ad-hoc): Policies, procedures and strategies are not formalized; activities are performed in an ad hoc, reactive manner.

2. Level 2 (Defined): Policies, procedures, and strategies are formalized and documented but not consistently implemented.

3. Level 3 (Consistently Implemented): Policies, procedures and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.

4. 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.

5. 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 OIG 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 of the Cybersecurity Framework functions (e.g., Protect, Detect) at the maturity level of their choosing, which allows for agency specific considerations to be factored in.. In FY 2021, we determined that control domains evaluated at the Consistently Implemented rating level may be considered “effective” when (1) no deficiencies are identified within the control domain and (2) there are no evaluations of a maturity level below Consistently Implemented for FISMA metric questions within the control domain.

Section 2
Conclusion and Enterprise-wide Recommendations

Section 2: Conclusion and Enterprise-wide Recommendations

2.1 Conclusions

Conclusion

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

Based on the results of our evaluation, 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 all the selected function areas: Identify, Protect, Detect, Respond and Recover.

Progress for FY 2021

As in prior year, this performance audit was conducted with the constraints of COVID-19. Thus, the audit procedures followed the FY 2020 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 a comparison from the FY 2020 and FY 2021 IG FISMA Metrics. Improvements in the overall posture were evident with the increase in maturity levels for individual metrics. Most notably, there were 17 additional metrics being assessed at the Managed and Measurable level from the prior year. The most significant of these increases was in our evaluation of the Identify, Protect, and Recover functional areas. In these functional areas, Risk Management, Identity and Access Management, Data Protection and Privacy, and Contingency Planning domains increased to Managed and Measurable level in FY 2021 versus the overall rating of Consistently Implemented in FY 2020.

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

- Improvements surrounding the reporting and monitoring of the PBGC POA&M Process.

Specifically, within the Identity and Access Management domain we noted that PBGC's cybersecurity program improvements supported an increased rating due to the following:

- Improvements surrounding overall workforce assessment knowledge.
- Improvements in management dashboards allow for greater insight into user status throughout onboarding.
- Improvements in management dashboards allow for increased visibility into existing SOD issues and role assignments.

Specifically, within the Data Protection and Privacy domain we noted that PBGC's cybersecurity program improvements supported an increased rating due to the following:

- Integration of Tabletop exercises with contingency planning by involving members of the security communications and backup/restore teams which also make up the breach response team.
- Improvements in workforce analysis to identify gaps associated with the DPP domain.

Specifically, within the Contingency Planning domain we noted that PBGC's cybersecurity program improvements supported an increased rating due to the following:

- Integration of Tabletop exercises with data protection and privacy.
- Improvements in the review of the contingency plans.

Table 2: FY 2020 and 2021 PBGC Maturity Levels

Maturity Level	FY 2020 IG FISMA Metrics	FY 2021 IG FISMA Metrics*
Ad-hoc	0	2
Defined	5	2
Consistently Implemented	22	4
Managed and Measurable	32	49
Includes SCRM metric scores which were not included in the FISMA program effectiveness conclusions for FY2022.		

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 several findings in PBGC's security program and consolidated them into each of the nine domains below.

Function	Identify		Protect				Detect	Respond	Recover
Domain	*Risk Management*	***Supply Chain Risk Management***	*Configuration Management*	*Identity & Access Management*	*Data Protection & Privacy*	*Security Training*	*ISCM*	*Incident Response*	*Contingency Planning*
OIG Assessed Maturity	Managed and Measurable (Level 4)	Defined (Level 2)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)

Function	Identify		Protect				Detect	Respond	Recover
Domain	*Risk Management*	***Supply Chain Risk Management***	*Configuration Management*	*Identity & Access Management*	*Data Protection & Privacy*	*Security Training*	*ISCM*	*Incident Response*	*Contingency Planning*
Change FY 2021 Audit vs. FY 2020	Increased One Level	New for FY2021	No Change	Increased One Level	Increased One Level	No Change	No Change	No Change	Increased One Level

2.3 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 is one domain, Risk Management, for evaluation within the IG metrics. 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 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.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2021 IG Assessment	Change from FY 2020 IG Assessment
Identify	Risk Management	Managed and Measurable	Increased One Level

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

- PBGC maintains a comprehensive and accurate inventory of its information systems and ensures that these information systems are subject to the monitoring processes defined within the organization's ISCM strategy *(metric 1)*
- PBGC utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets and ensures 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 *(metric 2)*

- PBGC utilizes its standard data elements/taxonomy to develop and maintain an up-to-date inventory of software assets and licenses and ensures that the 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 *(metric 3)*

- PBGC ensures the risk-based allocation of resources based on system categorization through collaboration and data-driven prioritization *(metric 4)*

- PBGC employs robust 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 *(metric 5)*

- PBGC consistently implements its security architecture across the enterprise, business process, and system levels. In addition, PBGC employs a software assurance process for mobile applications by leveraging Microsoft Intune capabilities. *(metric 6)*

- PBGC has defined the roles and responsibilities of stakeholders involved in cybersecurity risk management processes and those individuals are held accountable for consistently performing their roles and responsibilities effectively *(metric 7)*

- PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its POA&M activities and uses that information to make appropriate adjustments, as needed, to ensure that its risk posture is maintained *(metric 8)*

- PBGC utilizes a cybersecurity risk register and employs robust 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 *(metric 9)*

- 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 ensures that cybersecurity risk management information is integrated into ERM reporting tools, such as a governance, risk management, and compliance tool), as appropriate *(metric 10)*

Risk Management Finding

For the FY 2021 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 2021 IG Assessment	Change from FY 2020 IG Assessment
Identify	Supply Chain Risk Management	Defined	Not evaluated in the prior year.

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

- PBGC has defined and communicated an organization wide SCRM strategy *(metric 12)*
- Defined procedures for detecting and preventing counterfeit components from entering its information systems *(metric 15)*.

Supply Chain Risk Management Findings and Recommendations

For the FY 2021 assessment year, the following findings were identified with PBGC's supply chain risk management program:

- We observed that prior year issue (NFR IT-2020-006-FISMA-RM) remained unresolved related to the implementation of a supply chain risk management plan:

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

- PBGC should develop and implement a supply chain risk management plan to address supply chain risks with respect to information systems and system components. Further, PBGC should educate the acquisition workforce on threats, risk and required security controls for acquired IT components. (2021-05-01)

PBGC Response:

PBGC concurs with this recommendation. The Enterprise Cybersecurity Department (ECD) implemented the Cyber Supply Chain Risk Management (C-SCRM) Strategy in August 2021. ECD plans to fully address the recommendation in FY2022 and will provide supporting documentation to the OIG.

2.4 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. Our overall assessment of this function was "Effective."

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2021 IG Assessment	Change from FY 2020 IG Assessment
Protect	Configuration Management	Managed and Measurable	No change
	Identity and Access Management	Managed and Measurable	Increased One Level
	Data Protection and Privacy	Managed and Measurable	Increased One Level
	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 has allocated resources in a risk-based manner for stakeholders to effectively perform information system configuration management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 17)*
- PBGC has defined and consistently implemented an organization-wide configuration management plan and has integrated its plan with its risk management and continuous monitoring programs. Further, the organization utilizes lessons learned in implementation to make improvements to its plan *(metric 18)*
- PBGC has consistently implemented its policies and procedures for managing the configurations of its information systems. Further, the organization utilizes lessons learned in implementation to make improvements to its policies and procedures. PBGC also employs automated mechanisms to detect unauthorized hardware, software, and

firmware on its network and take immediate actions to limit any security impact *(metric 19)*

- PBGC employs automation to help maintain an up-to-date, complete, accurate, and readily available view of the security configurations for all information system components connected to the organization's network *(metric 20)*

- PBGC centrally manages its flaw remediation process and utilizes automated patch management and software update tools for operating systems, where such tools are available and safe *(metric 21)*

- PBGC ensures that its trusted internet connections (TIC) implementation remains flexible and that its policies, procedures, and information security program are adapting to meet the security capabilities outlined in the TIC initiative. Further, PBGC monitors and reviews the implemented TIC 3.0 use cases to determine effectiveness and incorporate new/different use cases *(metric 22)*

- PBGC monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its change control activities and ensures that data supporting the metrics is obtained accurately, consistently and in a reproducible format. Further, PBGC implements defined security responses if baseline configurations are changed in an unauthorized manner *(metric 23)*

- PBGC has developed, documented, and publicly disseminated a comprehensive VDP, addressing the following: The systems in scope, types of testing allowed, reporting mechanisms, timely feedback, and remediation. In addition, PBGC has updated its vulnerability disclosure handling procedures to support the implementation of its VDP *(metric 24)*

Configuration Management Finding and Recommendations

For the FY 2021 assessment year, the following findings were identified with PBGC's configuration management domain:

- We observed that prior year issue (NFR IT-2020-013-FISMA-VAPT) remained unresolved related to the implementation of a strong cryptological ciphers.

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

- Harden the affected servers' cipher suites to avoid the use of weak ciphers and RC4 ciphers, in accordance with the vendor's security leading practices. (2021-05-02)

Further, we recommend that PBGC management should continue with their implementation plan to address the prior year issue identified by OIG which were identified in planning to continue to impact the configuration management domain related to 2016-01-04 and implement

an improved website vulnerability management program to address security deficiencies in the development of websites.

PBGC Response:

PBGC concurs with these recommendations. ITIOD plans to address both in FY2022 and will provide supporting documentation to the OIG.

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 ensures that individuals are performing the roles and responsibilities that have been defined across the organization and that resources are allocated in a risk-based manner for stakeholders to effectively implement identity, credential, and access management activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 26)*

- PBGC has developed and consistently implements a comprehensive ICAM policy, strategy, process, and technology solution road map and is on track to meet milestones. PBGC integrates its ICAM strategy and activities with its enterprise architecture and the Federal ICAM architecture and uses automated mechanisms, where appropriate, to manage the effective implementation of its ICAM policies, procedures, and strategy *(metric 27)*

- PBGC ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access and rescreened periodically. Further, PBGC employs automation to centrally document, track, and share risk designations and screening information with necessary parties *(metric 28)*

- PBGC ensures that access agreements for individuals are completed prior to access being granted to systems and are consistently maintained thereafter. PBGC uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized *(metric 29)*

- PBGC has consistently implemented strong 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 utilize strong authentication mechanisms to authenticate to applicable organizational systems *(metric 30)*

- PBGC has planned for the use of strong 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 *(metric 31)*

- PBGC ensures that its processes for provisioning, managing, and reviewing privileged accounts are consistently implemented across the organization. The organization limits the functions that can be performed when using privileged accounts, limits the duration that privileged accounts can be logged in, limits the privileged functions that can be performed using remote access, and ensures that privileged user activities are logged and periodically reviewed *(metric 32)*

- PBGC ensures that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 30 minutes (or less), and that remote users' activities are logged and reviewed based on risk. Further, PBGC ensures that end-user devices have been appropriately configured prior to allowing remote access and restricts the ability of individuals to transfer data accessed remotely to unauthorized devices *(metric 33)*

Identity and Access Management Findings and Recommendations

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

- Controls and processes related to administrative accounts and privileged functions had weaknesses that allowed for direct compromise of accounts and systems. These issues may indicate a gap in security policy or configuration, processes, or procedures as they relate specifically to privileged access management. (NFR IT 2021-001-FISMA-VAPT)

- Security settings and configurations were found on systems on the network that allowed escalation of unauthorized access and/or privileges. These issues are typically related to weak baseline hardening policies and guidelines, lack of environmental awareness, a lack of technical capability or support, or even intentionally insecure settings to support legacy services. (NFR IT 2021-001-FISMA-VAPT)

- We observed that prior year issues (NFR IT-2021-001-OIT-SOD and NFR IT-2021-002-OBA-SOD) remained unresolved related to the implementation of segregation of duty controls.

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

- PBGC should create organization-wide policies surrounding establishment of passwords and password protection to ensure constant implementation of new technology and standards. (2022-07-01)

- PBGC should complete mitigations against password guessing attacks. (2022-07-02)

- PBGC should schedule periodic password resets to prevent previously obtained or compromised credentials from being re-used on PBGC domains. (2022-07-03)

- Develop and update segregation of duty matrices to reflect the risk of multiple role assignments based on the current business operations of PBGC within the CMS system. (2021-02-05)

- Review existing role assignments based on existing OBA conflict matrices and updated CMS segregation of duty matrices for existing conflicts and remediate them as appropriate. (2021-02-06)

- PBGC should enhance existing monitoring controls to mitigate risks associated with required role assignments that violate separation of duty requirements. (2021-02-07)

- PBGC should enhance existing monitoring controls to mitigate risks associated with required role assignments that violate separation of duty requirements. (2021-02-10)

Further, we recommend that PBGC management should continue with their implementation plan to address the prior year issues identified by OIG which were identified in planning to continue to impact the Identity and Access Management domain related to 2015-09-15, 2020-05-02 and 2020-05-03 around improvements to their personnel security program and implement the following recommendations:

- PBGC should develop, document and implement a process for the timely assessment of employees and contractors transferred or promoted to a new position or role to determine whether the risk-level has changed. (2015-09-15)

- PBGC should improve processes and implement oversight to ensure timeliness of background investigations to be completed for federal employees and contractors. (2020-05-02)

- PBGC should update directives, policies, and procedures to reflect current personnel security processes for the timely processing of background investigations. (2020-05-03)

PBGC Response

PBGC concurs with these findings and recommendations. With regards to recommendation 2022-01-02, ITIOD will fully evaluate the recommendation for technical feasibility, cost, and schedule. ITIOD plans to address all of these recommendations in FY2022 and will provide supporting documentation to the OIG.

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 have the following in place:

- PBGC consistently implements its privacy program by dedicating appropriate resources to the program, maintaining an inventory of the collection and use of PII, conducting and maintaining privacy impact assessments and system of records notices for all applicable systems, and reviewing and removing unnecessary PII collections on a regular basis *(metric 35)*

- 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 ensures that the security controls for protecting PII and other agency sensitive data, as appropriate, throughout the data lifecycle are subject to the monitoring processes defined within the organization's ISCM strategy *(metric 36)*

- 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 *(metric 37)*

- PBGC has defined, communicated, and consistently implemented its Data Breach Response Plan, including its processes and procedures for data breach notification. Further, a breach response team has been established that includes the appropriate agency officials. Further, PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its Data Breach Response Plan, as appropriate and ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format *(metric 38)*

- PBGC measures the effectiveness of its privacy awareness training program by obtaining feedback on the content of the training and conducting targeted phishing exercises for those with responsibility for PII. Additionally, the organization updates its program based on statutory, regulatory, mission, program, business process, information system requirements, and/or results from monitoring and auditing *(metric 39)*

Data Protection and Privacy Findings and Recommendations

For the FY 2021 assessment year, the following findings were identified with PBGC's Data Protection and Privacy domain:

- We observed that prior year issue (NFR IT-2020-008-FISMA-DPP) remained unresolved related to the monitoring of internal disclosures of PII.

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

- PBGC should conduct an analysis to determine if the current PBGC internal network monitoring capabilities are sufficient to fully support their insider threat program, specifically around the monitoring and disclosure of PII and sensitive banking information. Where appropriate PBGC should deploy additional toolsets to monitor internal transmissions of PII and sensitive banking information for insider threat behavior analytic modeling. (2021-05-07)

- PBGC should conduct a risk assessment to consider the inclusion of the AU-13 optional control requirements for monitoring information disclosures by internal employees. (2021-05-08)

PBGC Response

PBGC concurs with these recommendations. ITIOD plans to address both in FY2022 and will provide supporting documentation to the OIG.

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 ensures resources (people, processes and technology) are allocated in a risk-based manner for stakeholders to consistently implement security awareness and training responsibilities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 41)*

- 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 *(metric 42)*

- PBGC has defined and consistently implemented its organization-wide security awareness and training strategy and plan. Further, PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its security awareness and training strategies and plans. The organization ensures that data supporting metrics are obtained accurately, consistently and in a reproducible format *(metric 43)*

- PBGC defined and tailored its security awareness policies, procedures and ensures that its security awareness policies and procedures are consistently implemented. Further, PBGC measures the effectiveness of its awareness training program by, for example, conducting phishing exercises and following up with additional awareness or training, and/or disciplinary action, as appropriate *(metric 44)*

- PBGC has defined its security training policies, procedures and ensures that its security training policies and procedures are consistently implemented. Further, PBGC obtains feedback on its specialized security training content and processes and makes updates to its program, as appropriate. In addition, the organization measures the effectiveness of its specialized security training program by, for example, conducting targeted phishing exercises and following up with additional training, and/or disciplinary action, as appropriate *(metric 45)*

Security Training Findings and Recommendations

For the FY 2021 audit year, there were no identified findings regarding the PBGC Security Training domain.

2.5 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, which are three principal documents in a security authorization package.

Cybersecurity Framework Function Area	IG FISMA Domain	FY 2021 IG Assessment	Change from FY 2020 IG Assessment
Detect	ISCM	Managed and Measurable	No change

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 ensures that data supporting metrics are obtained accurately, consistently and in a reproducible format *(metric 47)*

- PBGC-developed ISCM policies and procedures have been consistently implemented for the specified areas and consistently captures lessons learned to make improvements to the ISCM policies and procedures. PBGC ensures individuals are performing the roles and responsibilities that have been defined across the organization and that resources are allocated in a risk-based manner for stakeholders to effectively implement ISCM activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 48)*

- 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 *(metric 49)*

- PBGC has defined and consistently captures qualitative and quantitative performance measures on the performance of its ISCM program. Further, PBGC integrates metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations and security domains *(metric 50)*

ISCM Findings and Recommendations

For the FY 2021 audit year, there were no identified findings regarding the PBGC ISCM domain.

2.6 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 2021 IG Assessment	Change from FY 2020 IG Assessment
Respond	Incident Response	Managed and Measurable	No change

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

- PBGC monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans and strategies, as appropriate. The organization ensures that data supporting metrics is obtained accurately, consistently, and in a reproducible format *(metric 52)*
- PBGC ensures individuals are performing the roles and responsibilities that have been defined across the organization. Further, PBGC allocates their resources in a risk-based manner for stakeholders to effectively implement incident response activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 53)*
- PBGC utilizes 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 *(metric 54)*
- 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 ensures that data supporting metrics are obtained accurately, consistently, and in a reproducible format *(metric 55)*
- PBGC consistently shares information on incident activities with internal stakeholders and ensures incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders *(metric 56)*
- PBGC utilizes Einstein 3 Accelerated to detect and proactively block cyber-attacks or prevent potential compromises *(metric 57)*
- PBGC consistently implements its defined incident response technologies in the specified areas. In addition, PBGC evaluates the effectiveness of its incident response technologies and adjusts configurations and toolsets, as appropriate *(metric 58)*

Incident Response Findings and Recommendations

For the FY 2021 audit year, there were no identified findings regarding the PBGC Incident Response domain.

2.7 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 2021 IG Assessment	Change from FY 2020 IG Assessment
Recover	Contingency Planning	Managed and Measurable	Increased One Level

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

- PBGC has ensured that individuals are performing the roles and responsibilities that have been defined across the organization. Further, PBGC has allocated their resources in a risk-based manner for stakeholders to effectively implement system contingency planning activities. Further, stakeholders are held accountable for carrying out their roles and responsibilities effectively *(metric 60)*

- PBGC consistently implements its defined information system contingency planning policies, procedures, and strategies. Further, PBGC ensures that the results of organizational and system level BIA's are integrated with enterprise risk management processes, for consistently evaluating, recording, and monitoring the criticality and sensitivity of enterprise assets *(metric 61)*

- PBGC integrates metrics on the effectiveness of its information system contingency plans with information on the effectiveness of related plans, such as organization and business process continuity, disaster recovery, incident management, insider threat implementation and occupant emergency, as appropriate to deliver persistent situational awareness across the organization *(metric 62)*

- 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 *(metric 63)*

- PBGC consistently implements its processes, strategies, and technologies for information system backup and storage. Further, PBGC ensures that its information system backup and storage processes, including use of alternate storage and processing sties, and related supply chain controls, are assessed, as appropriate, as part of its continuous monitoring program *(metric 64)*

- PBGC communicates to relevant stakeholders, and the organization has ensured that the data supporting the metrics is obtained accurately, consistently and in a reproducible format *(metric 65)*

Contingency Planning Findings and Recommendations

For the FY 2021 audit year, there were no identified findings regarding the PBGC Contingency Planning domain.

Section 3
Appendices

Appendix A
Audit Scope and Methodology

Section 3: Appendices

Appendix A: Audit Scope and Methodology

Scope

In tandem with the 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 developed a Notification 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 internal assessments performed on behalf of PBGC management that had a similar scope to the FY 2021 IG FISMA metrics. Incorporated the results as part of the FY 2021 IG FISMA metrics.
- Inspected results from GAO and OIG audits and reports that had a similar scope to the FY 2021 IG FISMA metrics. Incorporated the results as part of the FY 2021 IG FISMA metrics and identified related findings and recommendations from prior year assessments within this report that continue to impact the subject matter.

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

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). PBGC Office of Information Security, High Value Asset Program Policy (March 2018).
- PBGC Information Security Risk Management Framework (RMF) Process (February 2021).
- PBGC Infrastructure Configuration Management Plan (ICMP) (July 14, 2021).
- PBGC Enterprise Continuous Monitoring (ECM) Strategy and Plan (January 2021).
- PBGC Enterprise Architecture Configuration Management Plan (March 2016)
- PBGC Configuration Management Standard Operating Procedure (SOP) (August 4, 2021).
- PBGC Office of Information Technology Data Loss Prevention Standard Operating Procedure (May 22, 2020).
- PBGC Security Awareness Training 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 22, 2015).
- 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-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (October 16, 2017).
- US-CERT Federal Incident Notification Guideline

Appendix C
PBGC Management Response

Appendix C: PBGC Management Response

Management Response to FY 2021 FISMA Report.

PBGC
Protecting America's Pensions
Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

Office of the Director

January 27, 2022

MEMORANDUM

To: Nicholas J. Novak
Inspector General

From: Gordon Hartogensis
Director

Gordon Hartogensis
Digitally signed by Gordon Hartogensis
Date: 2022.01.27 13:46:25 -05'00'

Subject: Response to OIG's Draft Fiscal Year 2021 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 2021. Your office's work on this is sincerely appreciated.

It was helpful to receive the associated Notices of Findings and Recommendations (NFRs) ahead of this report. This allowed for expeditious initiation of planning and remediation activities, which will lead to mutually desirable outcomes for the agency and the OIG.

Management 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. Our planned corrective actions for the financial statement related recommendations were included in our response to the *Independent Auditor's Combined Audit Report for the FY 2021 Financial Statement Audit* (AUD-2022-03, issued November 15, 2021). 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. 2022-07-01: (NFR IT-2021-001-FISMA-VAPT) PBGC should create organization -wide profiles surrounding establishment of passwords and password protection to ensure constant implementation of new technology and standards.

PBGC Response: PBGC concurs with this recommendation. The Office of Information Technology (OIT) will coordinate with the different business application teams to update the passwords for the affected service accounts or deprovision the accounts if they are no longer required. Additionally, OIT will apply Group Policy Object (GPO) policies to ensure password compliance with PBGC policy.

Target Completion Date: 6/30/2022

OIG Recommendation No. 2022-07-02: (NFR IT-2021-001-FISMA-VAPT) PBGC should complete mitigations against password guessing attacks.

PBGC Response: PBGC concurs with this recommendation. The Information Technology Infrastructure Operations Department (ITIOD) will fully evaluate the recommendations for technical feasibility, cost, and schedule. Passwords will be changed to comply with current complexity and cryptographic standards, as feasible.

Target Completion Date: 6/30/2022

OIG Recommendation No. 2022-07-03: (NFR IT-2021-001-FISMA-VAPT) PBGC should schedule periodic password resets to prevent previously obtained or compromised credentials from being re-used on PBGC domains.

PBGC Response: PBGC concurs with this recommendation. Additionally, OIT will apply GPO policies to ensure password compliance with PBGC policy.

Target Completion Date: 6/30/2022

Appendix D
Additional Details Related to IT NFRs

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	Criteria	Effect	Recommendation Number
NFR IT-2020-006-FISMA-RM	PBGC did not have a documented supply chain risk management plan that formally documented requirements.	NIST Special Publication 800-53, Revision 4 Control PM-9 Risk Management Strategy and Control SA-12 Supply Chain Protection	PBGC is exposed to the risk of supply chain disruption and is not able to effectively protect information systems and information system components, prior to taking delivery of such systems/components.	Recommendation Number 2021-05-01
NFR IT-2020-013-FISMA-VAPT	Management did not securely configure or review external-facing website security configurations for known weaknesses and remediate them as appropriate.	NIST Special Publication 800-53, Revision 4 Control RA-5 Vulnerability Scanning	An attacker can use the txt file to gain potentially sensitive information regarding the web server directory structure. This information could allow an attacker to understand the layout of the server and can be used to craft targeted attacks against the server later.	Recommendation Number 2021-05-02
NFR IT-2020-008-FISMA-DPP	PBGC management stated that increased emphasis was placed on protecting its PII and other agency sensitive data against external transmission due to the higher level of risk, and the same level of rigor has not been applied over unauthorized internal disclosure.	PBGC Cybersecurity and Privacy Catalog (CPC), Section 3.2 Privacy Controls Table 8 Use Limitation (UL) UL-1 Internal Use	PBGC is exposed to the risk that PII information can be maliciously disclosed with internal parties without detection and/or monitoring.	Recommendation Number 2021-05-07 and 2021-05-08

IT NFR Number	Cause	Criteria	Effect	Recommendation Number
NFR IT-2021-001-FISMA-VAPT	Management did not securely configure, or review processes and configurations associated with privileged access and administrative accounts.	NIST Special Publication 800-53, Revision 4 Control AC-2 Account Management Control AC-2 Access Enforcement	Weak passwords on system accounts could lead to unauthorized access to privileged domain roles and allow for inappropriate access across the PBGC network.	Recommendation Number 2022-07-01, 2022-07-02 and 2022-07-03
NFR IT-2021-001-OIT-SOD	Management had not developed a cross application role assignment for PBGC systems. Additionally, management had misconfigured their rulesets, which failed to identify all known all violations appropriately so that PBGC management could take appropriate follow-up actions.	NIST Special Publication 800-53, Revision 4 Control AC-5 Separation of Duties	If management does not identify and monitor segregation of duties conflicts, considering both IT and business process roles and activities, the risk increases that users could obtain inappropriate access resulting in the potential for unauthorized activity.	Recommendation Number 2021-02-07 and 2021-02-10
NFR IT-2021-002-OBA-SOD	Management did not completely and accurately document user roles conflicts within the Segregation of Duties matrices for the CMS systems. For roles with risk conflict identified, management did not submit complete documentation to accurate capture the risk acceptance of all known role conflicts for the identified users.	NIST Special Publication 800-53, Revision 4 Control AC-5 Separation of Duties	If management does not identify and monitor segregation of duties conflicts, considering both IT and business process roles and activities, the risk increases that users obtain inappropriate access resulting in the potential for unauthorized activity.	Recommendation Number 2021-02-05 and 2021-02-06

IT NFR Number	Cause	Criteria	Effect	Recommendation Number
Note: Findings and Recommendations associated with the Configuration Management domain over an improved website vulnerability management program (2016-01-04) and with the Identity and Access Management domain over personnel security program improvements (2020-05-02, 2020-05-03, and 2015-09-15) were issued by the PBGC OIG and utilized during our scoping and planning process to identify prior year observations or findings that continue to impact the subject matter. While evaluated to continue to be open by our team, we conducted no additional testing over these findings and planned our audit procedures with these deficiencies accordingly. As such, management should refer to prior NFRs for cause, criteria, and effect information.				

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.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

2011-3646362
ED None

ey.com