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 2020

Report No. AUD-2021-5
January 21, 2021

Office of Inspector General

January 21, 2021

MEMORANDUM

TO: Gordon Hartogensis
Director

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

SUBJECT: PBGC's Implementation of the Federal Information Security Modernization Act of 2014 for FY 2020 (AUD-2021-5)

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 17 new FISMA-related recommendations. Six were issued in the financial statement audit report and 11 were issued in this report. PBGC agreed with the 11 new recommendations in this report and previously agreed with the 6 recommendations in the financial statements audit 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
Patricia Kelly
Alice Maroni
Karen Morris
Andy Banducci
Paul Chalmers
Frank Pace
Latreece Wade

# Pension Benefit Guaranty Corporation

## Federal Information Security Modernization Act Report

January 15, 2021

Building a better working world

Building a better
working world

Ernst & Young LLP
1775 Tysons Blvd
Tysons, VA 22102

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

# Report of Independent Auditors on Pension Benefit Guaranty Corporation's Implementation of the Federal Information Security Modernization Act of 2014 for Fiscal Year 2020 Based on a Performance Audit Conducted in Accordance with *Government Auditing Standards*

Mr. Nicholas Novak
Acting 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, 2020, as defined in the FY 2020 Inspector General FISMA Reporting Metrics.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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. The nature, timing, and extent of the procedures selected depend on our judgment. 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.

Ernst & Young LLP

January 15, 2021

# Report in Brief

Date: January 15, 2021

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, 2020, 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-defined 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 2020

## What we found

Overall, through the evaluation of FISMA metrics, it was determined that PBGC's information security program was "Not Effective." This determination was made based on (1) the evaluation of PBGC not meeting a "Managed and Measurable" maturity level for Identify, Protect, and Recover functional areas; (2) the deficiencies identified within the Identify and Protect functional areas; (3) the lack of Managed and Measurable ratings to mitigate the Consistently Implemented ratings in control domains that were further evaluated for effectiveness; and (4) the evaluation of a maturity level below Consistently Implemented for individual metric questions. Specific recommendations were also provided to PBGC management for their awareness.

However, progress continues to be made to sustain cybersecurity maturity across all FISMA domains. We noted an increased maturation of the configuration management and security training domains. We identified opportunities where PBGC can strengthen its overall information security program. Weaknesses continue to persist in functional areas of Risk Management, Identity & Access Management, Data Protection & Privacy, and Security Training.

## What we recommend

We recommend that PBGC further strengthen its cybersecurity program and enhance information security controls at PBGC.

PBGC should implement quantitative and qualitative performance measures to track trends and address common risk across PBGC. Specifically, PBGC should complete their "to-be ICAM Architecture" to ensure that they are meeting all monthly goals, as well as leverage the Workforce GAP Assessment to ensure all business continuity aspects are covered. Further, we recommend PBGC develop a supply chain management strategy to strengthen the risk management domain. Tabletop exercises in the data protection and privacy domain should be implemented and analyzed to meet requirements for effective maturity.

PBGC's FISMA program should address gaps between the current maturity levels to the PBGC-defined effective maturity level for each of the National Institute of Standards and Technology (NIST) cybersecurity framework (CSF) function areas. We also recommend PBGC ensure that their Cybersecurity Maturity strategy advances to meet an effective state across all functional areas.

# 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 implementation of the Federal Information Security Modernization Act of 2014 (FISMA) as of September 30, 2020, 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 FISMA 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 2020 IG FISMA reporting metrics, issued April 9, 2020, 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 2020 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 2020 metrics also mark a continuation of the work that OMB, DHS and CIGIE undertook in the past five years to move the IG assessments to a maturity model approach.

For FY 2020, updates were made to the IG FISMA questions, as reported in the FY 2020 IG FISMA Reporting Metrics Version 1.3, dated April 9, 2020, which include the following:

- The FY 2020 CIO FISMA Metrics, OMB Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, and DHS' Binding Operational Directive 18-02, *Securing High Value Assets*, have placed additional emphasis on the enhancement of the High Value Asset (HVA) program. As such, the FY 2020 IG FISMA Reporting Metrics include additional maturity indicators and criteria references regarding the evaluation of the effectiveness of agencies' HVA programs.

- On December 21, 2018, the Strengthening and Enhancing Cyber-Capabilities by Utilizing Risk Exposure Technology Act of 2018 (SECURE Technology Act) established new requirements for supply chain risk management. The FY 2020 IG FISMA Metrics have been updated to gauge agencies' preparedness in addressing these new requirements while recognizing that specific guidance will be issued at a later date.

The FY 2020 IG FISMA Reporting Metrics are grouped into eight 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 |
| **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 2020 IG FISMA Metrics, a series of metrics (or questions) was developed for each IG FISMA domain (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 functional areas (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.

# 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 "Not Effective," as it did not meet the criteria required to be assessed at a "Managed and Measurable" maturity level for all of the selected function areas: Identify, Protect, Detect, Respond and Recover.

### *Progress for FY 2020*

This performance audit was conducted with the constraints of COVID-19. Thus, audit procedures were revised 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. As such, FY 2019 and FY 2020 results may not be fully comparable.

Table 2 below provides a comparison from the FY 2019 and FY 2020 IG FISMA Metrics. Improvements in the overall posture were evident with the increase in maturity levels for individual metrics. Most notably, there were 21 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 Protect functional area. In that functional area, both Configuration Management and Security Training domains increased to Managed and Measurable level in FY 2020 versus the overall rating of Consistently Implemented in FY 2019.

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

- Collect additional feedback from the Annual Security and Privacy Awareness and Training
- Enhanced compliance process by excluding waivers
- Managed continuous automated compliance monitoring (CACM)
- Utilize role-based training (RBT) system-generated reporting via FedTalent
- Verification of RBT Training Status
- Conduct Cyber Security Awareness Week (CSAW)
- Improve dashboard reporting in Enterprise Risk Intelligence Quotient (ERIQ) dashboard

- Improve Phishing Exercise reporting in ERIQ dashboard
- Innovated use of technology for training due to COVID-19
- Usage of both qualitative and quantitative performance measures for training via ERIQ dashboard

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

- PBGC has clearly communicated roles and responsibilities of key stakeholders
- PBGC has performance measures to monitor the overall program, for example:
  - Maintain an average (monthly) aggregate configuration item (CI) baseline security compliance rate of 98.75% or better for all infrastructure components in areas of responsibility as measured by CACM
  - Achieve 99% timely remediation (within 30 days of the first detection) when an individual CI falls below the min. CI baseline compliance threshold by correcting the configuration issue, removing the CI, or documenting a RA for areas of responsibility

Table 2: FY 2019 and 2020 PBGC Maturity Levels

| Maturity Level | FY 2019 IG FISMA Metrics | FY 2020 IG FISMA Metrics |
|---|---|---|
| **Ad-hoc** | 1 | 0 |
| **Defined** | 20 | 5 |
| **Consistently Implemented** | 27 | 22 |
| **Managed and Measurable** | 11 | 32 |

## 2.2 Enterprise-wide Recommendations

***FY 2020 Recommendations***

PBGC should commit to creating and implementing a Cybersecurity Maturity Strategy to advance the cybersecurity program from its current maturity state to an effective state across PBGC. This strategy should include the following focusing on improving the following areas:

### Risk Management

- Collaborate to ensure that a value-driven assessment is used to determine resources for assets.
- Track trends in plan of action and milestones (POA&Ms) by analyzing qualitative and quantitative performance measures to better allocate resources based on common risk across the PBGC Enterprise.

### Configuration Management

- Implement operating procedures to be used on a daily basis that utilize trend analysis of vulnerability assessments and flaw remediation.

### Identity and Access Management

- Ensure completion of the Identity Credential and Access Management (ICAM) Roadmap to help enable PBGC achieve their “to-be ICAM Architecture.”

- Centrally track risk designations within PBGC and not solely through USAccess.

### Security Training

- Continue to include phishing considerations within ongoing security training requirements.

### ISCM

- Ensure full compliance, specifically, in the automation of POA&Ms status and incident response, where PBGC should implement monitoring to instantly identify various incidents and integrate them into the POA&M development.

- Utilize ERIQ Dashboards to assist with the ongoing adaption of ISCM policies and procedures to ensure that PBGC is following the most up-to-date process for the ISCM domain.

- Ensure that the Enterprise Continuous Monitoring (ECM) Program adapts and updates information on a real-time basis.

### Incident Response

- Ensure that levels of authority are adjusted to respond to risk associated with the Incident Response domain to ensure that resources are allocated where needed on an ongoing basis.

- Maintain equivalent profiling on the network.

- Include key aspects such as application firewalls, intrusion detection, malware detection, and qualitative metrics in the ERIQ Dashboards.

### Contingency Planning

- Ensure that the Workforce GAP Assessment covers business continuity aspects.

# Section 3
# Cybersecurity Framework Domain Findings and Recommendations

# Section 3: Cybersecurity Framework Domain Findings and Recommendations

## 3.1 Summary

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 eight domains below.

| Function | Identify | Protect | | | | Detect | Respond | Recover |
|---|---|---|---|---|---|---|---|---|
| Domain | *Risk Management* | *Configuration Management* | *Identity and Access Management* | *Data Protection and Privacy* | *Security Training* | *ISCM* | *Incident Response* | *Contingency Planning* |
| **OIG Assessed Maturity** | Consistently Implemented (Level 3) | Managed and Measurable (Level 4) | Consistently Implemented (Level 3) | Consistently Implemented (Level 3) | Managed and Measurable (Level 4) | Managed and Measurable (Level 4) | Managed and Measurable (Level 4) | Consistently Implemented (Level 3) |
| **Change FY 2020 Audit vs. FY 2019** | No Change | Increased One Level | No Change | No Change | Increased One Level | No Change | No Change | No Change |

## 3.2 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 "Not 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 2020 IG Assessment | Change from FY 2019 IG Assessment |
|---|---|---|---|
| **Identify** | Risk Management | Consistently Implemented | No change |

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

- PBGC ensures that the information systems included in its inventory are subject to the monitoring processes defined within the organization's ISCM strategy.
- PBGC has defined priority levels for its information systems and considers risks from the supporting business functions and mission impacts.
- PBGC has performed an organization-wide security and privacy risk assessment. Risk management policies, procedures, and strategy have been developed and communicated across the organization. The strategy clearly states risk management objectives in specific and measurable terms.
- PBGC has ensured that individuals are performing the roles and responsibilities that have been defined across the organization.
- 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.
- PBGC has defined and communicated policies and procedures for system-level risk assessments and security control selections. In addition, PBGC has developed a tailored set of baseline controls and provides guidance regarding acceptable risk assessment approaches.
- PBGC employs robust diagnostic and reporting frameworks, including dashboards that facilitate a portfolio view of interrelated risks across the organization. The dashboard presents qualitative and quantitative metrics that provide indicators of risk.
- PBGC ensures that specific contracting language and SLAs are consistently included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services. Further, the organization obtains sufficient assurance, through audits, test results, or other forms of evaluation, that the security controls of systems or services provided by contractors or other entities on behalf of the organization meet FISMA requirements, OMB policy and applicable NIST guidance.
- PBGC has identified and defined its requirements for an automated solution that provides a centralized, enterprise-wide view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels and management dashboards.

### *Risk Management Finding*

The following finding was identified with PBGC's risk management program:

- PBGC did not have a documented supply chain risk management plan needed to support an effective risk management process [*NFR IT-2020-006-FISMA-RM* see appendix D for additional details].

PBGC should consider the following recommendations:

- 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 OCIO Response**

*PBGC RESPONSE from NFR IT-2020-006-FISMA RM*

ECD concurs with the finding and recommendations listed above. PBGC will coordinate with relevant stakeholders to create a Supply Chain Risk Management strategy and has created POA&M 3256 to address these findings.

### 3.3 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 "Not Effective."

| Cybersecurity Framework Function Area | IG FISMA Domain | FY 2020 IG Assessment | Change from FY 2019 IG Assessment |
|---|---|---|---|
| Protect | Configuration Management | Managed and Measurable | Increase |
| | Identity and Access Management | Consistently Implemented | No change |
| | Data Protection and Privacy | Consistently Implemented | No change |
| | Security Training | Managed and Measurable | Increase |

***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.

- PBGC has 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.

- 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 employs automated mechanisms (such as application approved listing and network management tools) to detect unauthorized hardware, software, and firmware on its network and take immediate actions to limit any security impact.

- 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.

- 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.

- 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 TIC 3.0, including the use of TIC Use Case requirements, as appropriate, for scenarios in which traffic may not be required to flow through a physical TIC access point.

- 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.

### *Configuration Management Finding*

The following finding was identified with PBGC’s configuration management program:

- Upon completion of the internet vulnerability and penetration assessment, it was noted that a PBGC txt file was publicly accessible in the root directory as well as multiple hosts that supported vulnerable versions of secure socket layer/ transport layer security [*NFR IT-2020-013-FISMA-VAPT* see appendix D for additional details].

- PBGC has documented formal policies and procedures to identify, track and remediate vulnerabilities. However, there were vulnerabilities that were misidentified on the vulnerability tracking reports, which lead to vulnerabilities not being formally tracked [*NFR IT-2020-014* see appendix D for additional details].

### *Configuration Management Recommendation*

PBGC should consider the following recommendations:

- 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).
- Consider sanitizing the .txt file to not include any sensitive directories or files using the disallow directive. If possible, replace the use of the .txt file with the robots meta tag on specific pages that should be excluded from search engine indices (2021-05-03).
- Further, we recommend that PBGC management should continue with their implementation plan to address the prior year issue that was identified related to 2016-01-04: Implement an improved website vulnerability management program to address security deficiencies in the development of websites.
- PBGC management should correct the deficiencies in their vulnerability reporting and tracking process to identify source machine/IP and plug-in IDs for critical vulnerabilities with their original report date versus relying upon the first report date identified in their vulnerability tracking report (2021-05-04).

### PBGC OCIO Response

*PBGC RESPONSE From PBGC Security Assessment Report*

PBGC concurs with the OIG assessment and has completed the appropriate remediation activities. On October 1, 2020, OIT coordinated with the Communications Outreach & Legislative Affairs (COLA) Web Team to ensure that no .txt files are now being referenced on the pbgc.gov website's robots.txt file. The existing .php files are required for Drupal web content management framework to operate correctly. All .php files, however, require authentication and specific administrative rights to access and use, so there is no real risk of exposure or compromise. PBGC concurs with the OIG assessment and will be working with the different business units to disable TLS 1.0 where possible and perform risk assessment appropriately.

*PBGC RESPONSE from NFR IT-2020-014*

IT Infrastructure Operations Department (ITIOD) concurs with this finding. ITIOD had already made improvements to its vulnerability tracking process in the months following the auditor's observations and has further plans, already in motion, to further improve vulnerability tracking and reporting.

### *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.
- PBGC is consistently implementing its ICAM strategy and is on track to meet milestones. The strategy encompasses the entire organization, aligns with the Federal Information System Controls Audit Manual and continuous diagnostics and mitigation (CDM) requirements, and incorporates applicable federal policies, standards, playbooks and guidelines.
- PBGC has developed, documented, and disseminated its policies and procedures for ICAM. Policies and procedures have been tailored to the organization's environment and include specific requirements.
- PBGC ensures that all personnel are assigned risk designations, appropriately screened prior to being granted system access and rescreened periodically.
- PBGC uses automation to manage and review user access agreements for privileged and non-privileged users. To the extent practical, this process is centralized.
- PBGC ensures all non-privileged and privileged users utilize strong authentication mechanisms to authenticate to applicable organizational systems.
- 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.
- 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.

### *Identity and Access Management Findings*

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

- Segregation of duty rule sets were not designed effectively to mitigate weaknesses in PBGC logical access authorizations to IT systems supporting financial reporting [NFR IT-2020-004-ONR-SOD see appendix D for additional details].
- User roles in supporting applications did not reconcile to the identity management system utilized by PBGC to manage segregation of duty conflicts within the corporation [NFR IT-NFR IT-2020-003-OIT-SOD, 2020-005-FOD-SOD and NFR IT-2020-011-OBA-SOD see appendix D for additional details].

- A user-maintained access to an IT system supporting financial reporting that constituted a segregation of duties risk, without appropriate monitoring or mitigating controls being implemented [NFR IT-2020-003-OIT-SOD see appendix D for additional details].

- PBGC user separation and access termination process did not include a review of user activity post termination date to determine if separated users were inappropriately accessing their logical account [*NFR IT-2020-001_PBGC-Termination* see Appendix D].

- Privileged user activity justification documented prior to usage was not a sufficient level of detail to support login and support management review of appropriate of that activity [*NFR IT-2020-007-FISMA-IAM* see appendix D].

### *Identity and Access Management Findings Recommendation*

- PBGC should review existing role assignments based on updated segregation of duty matrices for existing conflicts and remediate them as appropriate (2021-02-06).

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

- PBGC should implement preventative mechanisms within their enterprise account management provisioning process to restrict the ability to assign conflicting roles without elevated approvals (2021-02-08).

- PBGC should ensure the enterprise account management solution is synchronized with application roles assigned within the IT systems supporting the financial reporting environment (2021-02-09).

- PBGC should increasing the frequency of the periodic review of users with known separation of duties violation to determine management concurrence with the appropriateness of the access and their risk acceptance (2021-02-10).

- PBGC should 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 IT systems supporting the financial reporting environment (2021-02-05).

- PBGC should implement a modification to the PBGC access termination process to identify those separated employees and contractors who accessed their logical account or physically accessed PBGC facilities after their termination date. Further, once an instance has been identified PBGC should investigate this inappropriate access for reasonableness and capture details as a potential security incident (2021-05-05).

- PBGC should undertake efforts to train the user base on the level of detail required to gain access to CyberArk. Specifically, management should conduct a reasonable review of this activity against approved tickets or other documented, authorized procedures (2021-05-06).

**PBGC OCIO Response**

*PBGC RESPONSE from NFR IT-2020-003-OIT-SOD*

ITIOD concurs with the recommendations. ITIOD acknowledges that all PBGC systems must maintain a Segregation of Duties (SoD) conflict matrix for their individual systems and ensure it is adhered to, but it is ITIOD's intent to provide a common mechanism for all system owners to do so.

*PBGC RESPONSE from NFR IT-2020-005*

The Financial Operations Department agrees with the need to:

- Update the Consolidated Financial System (CFS) segregation of duty matrix to ensure it appropriately reflects the risk of multiple role assignments based on the current business operations of PBGC and based upon those updates reviewing existing user assignments and application monitoring controls for any necessary updates

- Formalize the preventative mechanism within the current CFS account management provisioning process to document the approvals associated with the assignment of multiple roles with elevated risk

*PBGC RESPONSE from NFR IT-2020-011*

Office of Benefits Administration (OBA) management concurs with this finding. This past year, OBA focused on maturing the SoD matrices for all the OBA systems. Fiscal year 2021 has a road map for continued focus on Access Management across OBA systems. This plan has action items and milestones to address each recommendation listed above.

*PBGC RESPONSE from NFR IT-2020-001*

ITIOD concurs with the recommendation. While PBGC has reliable procedures in place to block both logical and physical access to employees on their effective separation date/time, in the rare instances where a separation request is submitted after an employee or contractor has been terminated, PBGC will adjust its process to investigate any inappropriate access that may have occurred and if any is detected, open a security incident.

*PBGC RESPONSE from NFR IT-2020-007-FISMA-IAM*

ITIOD concurs with the recommendation. ITIOD has efforts underway to ensure users receive the training necessary to gain access to CyberArk. ITIOD will also plan to conduct a reasonableness review of this activity against approved tickets or other documented authorized procedures.

### *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.

- 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.

- 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.

- PBGC has defined and communicated 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.

- 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.

### *Data Protection and Privacy Findings*

The following findings were identified with PBGC's data protection and privacy program:

- PBGC has implemented security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data life cycle. These security controls include encryption of data at rest, encryption of data in transit, limitation of transfer to removable media and sanitation of digital media prior to disposal or reuse. However, PBGC has not implemented security controls over PII or other agency sensitive data to unauthorized internal disclosure [*NFR IT-2020-008-FISMA-DPP* see appendix D for additional details].

- PBGC was not able to provide evidence to demonstrate their Data Breach Response plan was operating effectively, specifically we noted that, PBGC has developed a Data Breach Response plan, however PBGC did not conduct any tabletop exercises or lessons learned for FY 20 [NFR IT-2020-009-FISMA-DPP see appendix D for additional details].

### *Data Protection and Privacy Recommendations*

PBGC should consider the following recommendations:

- 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).

- With the adoption of NIST 800-53 rev5, 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 should conduct a data breach tabletop exercise, as well as monitor and analyze qualitative and quantitative performance measures on the effectiveness of its exercise (2021-05-09).

### PBGC OCIO Response

*PBGC RESPONSE from NFR IT-2020-008-FISMA-DPP*

ITIOD concurs with these findings. ITIOD will conduct an analysis to determine if the current PBGC internal network monitoring capabilities are sufficient to fully support PBGC’s insider threat program, specifically around the monitoring and disclosure of PII and sensitive banking information. Where appropriate, technically feasible, and practical to do so, PBGC will deploy additional toolsets to monitor internal transmissions of PII and sensitive banking information for insider threat behavior analytic modeling.

*PBGC RESPONSE from NFR IT-2020-009-FISMA DPP*

Office of the General Counsel agrees with this recommendation. While a data breach tabletop was not conducted this fiscal year, this was due to unforeseen circumstances and is atypical of PBGC. We will continue to conduct tabletop exercises moving forward and anticipate closure of this recommendation by next fiscal year.

### *Security Training*

An effective IT security program cannot be established and maintained without giving a sufficient amount of 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.

- 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.

- 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.

- 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.

### *Security Training Findings*

The following finding was identified with PBGC's security awareness training program:

- PBGC maintains a Workforce Development Strategy and Plan, and also undergoes a Workforce Assessment. EY identified two dashboards, one from March and the other from July, demonstrating an ongoing evaluation of PBGC needs. However, in areas that PBGC has demonstrated that they do not have a required role, as listed within the GAP Assessment, we were unable to identify plans to implement over the upcoming years [NFR IT-2020-010-FISMA-ST see appendix D for additional details].

### *Security Training Recommendations*

PBGC should consider the following recommendations:

- PBGC should utilize the Workforce Assessment Dashboard to determine how to fill gaps through the training or hiring of additional staff or contractors, as well as prepare an estimated timeline to fill this requirement (2021-05-10).

- PBGC should also share the gaps in the Workforce Assessment Dashboard with hiring managers so that they can understand the gaps and vet applicants who have the knowledge, skills and abilities (KSAs) to perform needed cybersecurity tasks (2021-05-11).

**PBGC OCIO Response**

*PBGC RESPONSE from NFR IT-2020-010-FISMA-ST*

Enterprise Cybersecurity Department (ECD) acknowledges the recommendations provided and concurs with this NFR. To address these recommendations ECD has opened POA&M 3264 to establish a plan for addressing known gaps and new/existing and applicable work roles. ECD will collaborate with the Cybersecurity and Privacy Council to develop a Cybersecurity Work Role Plan for identifying critical cyber functions aligned with the NIST Nice Framework (NIST SP 800-181).

### 3.4 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 2020 IG Assessment | Change from FY 2019 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.

- PBGC-developed ISCM policies and procedures have been consistently implemented for the specified areas. The organization also 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.

- PBGC utilizes the results of security control assessments and monitoring to maintain ongoing authorizations of information systems, including the maintenance of system security plans.

- 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.

### ISCM Findings and Recommendations

For the FY 2020 assessment year, while there are no explicit findings regarding the PBGC ISCM domain, the enterprise recommendation captured above should be adopted by PBGC to demonstrate the overall effectiveness of their program.

## 3.5 Respond

The goal of the Respond function is to develop and implement the appropriate activities to take action 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 2020 IG Assessment | Change from FY 2019 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.

- PBGC ensures individuals are performing the roles and responsibilities that have been defined across the organization.

- PBGC utilizes its threat vector taxonomy to classify incidents and consistently implements its processes for incident detection, analysis and prioritization. In addition, the organization consistently implements and analyzes precursors and indicators generated by, for example, the following technologies: intrusion detection/prevention, security information and event management (SIEM), antivirus and anti-spam software, and file integrity checking software.

- PBGC manages and measures the impact of successful incidents and is able to quickly mitigate related vulnerabilities on other systems so that they are not subject to exploitation of the same vulnerability.
- PBGC ensures incident response metrics are used to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.
- PBGC utilizes Einstein 3 Accelerated to detect and proactively block cyber attacks or prevent potential compromises.
- PBGC consistently implements its defined incident response technologies in the specified areas. In addition, the technologies utilized are interoperable to the extent practicable, cover all components of the organization’s network, and have been configured to collect and retain relevant and meaningful data consistent with the organization’s incident response policy, procedures and plans.

#### Incident Response Findings and Recommendations

For the FY 2020 assessment year, while there are no explicit findings regarding the PBGC Incident Response domain, the enterprise recommendation captured above should be adopted by PBGC to demonstrate the overall effectiveness of their program.

### 3.6 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 “Not 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 2020 IG Assessment | Change from FY 2019 IG Assessment |
|---|---|---|---|
| **Recover** | Contingency Planning | Consistently Implemented | No change |

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.
- PBGC consistently implements its defined information system contingency planning policies, procedures and strategies. In addition, the organization consistently implements technical contingency planning considerations for specific types of systems, including, but not limited to, methods such as server clustering and disk mirroring. Further, the organization is consistently capturing and sharing lessons learned on the effectiveness of information system contingency planning policies, procedures, strategy and processes to update the program.
- PBGC incorporates the results of organizational and system level business impact analysis into strategy and plan development efforts consistently.
- 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.
- PBGC employs automated mechanisms to more thoroughly and effectively test system contingency plans.
- PBGC consistently implements its processes, strategies, and technologies for information system backup and storage.
- 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.

### Contingency Planning Findings and Recommendations

For the FY 2020 assessment year, while there are no explicit findings regarding the PBGC Contingency Planning domain, the enterprise recommendation captured above should be adopted by PBGC to demonstrate the overall effectiveness of their program.

# Section 4
# Appendices

# Appendix A
# Audit Scope and Methodology

# Section 4: Appendices

## 4.1 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 implementation of the 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 2020 IG FISMA metrics. Incorporated the results as part of the FY 2020 IG FISMA metrics.
- Inspected results from GAO and OIG audits and reports that had a similar scope to the FY 2020 IG FISMA metrics. Incorporated the results as part of the FY 2020 IG FISMA metrics.

We conducted these procedures in accordance with 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

## 4.2 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 25, 2020).
- PBGC Infrastructure Configuration Management Plan (ICMP) (July 30, 2019).
- PBGC Enterprise Continuous Monitoring (ECM) Strategy and Plan (January 2020).
- PBGC Enterprise Architecture Configuration Management Plan (March 2016)
- PBGC Configuration Management Standard Operating Procedure (SOP) (August 1, 2019).
- PBGC Office of Information Technology Data Loss Prevention Standard Operating Procedure (May 22, 2020).
- PBGC Security Awareness Training Procedure (February 2020).
- PBGC Information Security Policy Directive IM 05-02 (April 22, 2020).
- PBGC Security Incident Management Operational Procedure (September 30, 2019).
- PBGC Enterprise Continuity of Operations Plan (COOP) (May 22, 2020).
- 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

## 4.3 Appendix C: PBGC Management Response

Management Response to Draft FY 2020 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 7, 2021

MEMORANDUM

To: Nicholas J. Novak
Acting Inspector General

From: Gordon Hartogensis
Director

Gordon Hartogensis Digitally signed by Gordon Hartogensis
Date: 2021.01.08 12:42:10 -05'00'

Subject: Response to OIG's Draft Fiscal Year 2020 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 2020. 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 2020 Financial Statement Audit* (AUD-2021-02, issued December 9, 2020). 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
Andy Banducci
David Foley
Karen Morris
Frank Pace
Patricia Kelly
Paul Chalmers
Alice Maroni
Robert Scherer
Theodore J. Winter

**OIG Recommendation No. 2021-05-01: (NFR IT-2020-006 FISMA-RM)** 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 information technology (IT) components.

**PBGC Response:** PBGC concurs with this recommendation. The Enterprise Cybersecurity Department (ECD) will coordinate with relevant stakeholders to create a Supply Chain Risk Management strategy and has created Plan of Action and Milestones (POA&M) 3256 & 3276 to address these findings.

**Target Completion Date: 6/30/2022**

**OIG Recommendation No. 2021-05-02: (NFR IT-2020-013-FISMA-VAPT)** 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.

**PBGC Response:** PBGC concurs with this recommendation. The Information Technology Infrastructure Operations Department (ITIOD) will work to improve the affected servers' cipher suites to strengthen the encryption utilized.

**Target Completion Date: 6/30/2022**

**OIG Recommendation No. 2021-05-03: (NFR IT-2020-013-FISMA-VAPT)** Consider sanitizing the .txt file to not include any sensitive directories or files using the disallow directive. If possible, replace the use of the .txt file with the robots meta tag on specific pages that should be excluded from search engine indices.

**PBGC Response:** PBGC concurs with this recommendation, however ITIOD would like to mention that this recommendation has already been completed as noted in the *PBGC Security Assessment Report* (Report No. SR-2021-04, issued December 23, 2020). Additionally, other .txt files previously referenced in the robots.txt file were removed from the website.

**Target Completion Date: 6/30/2021**

**OIG Recommendation No. 2021-05-04: (NFR IT-2020-014)** PBGC management should correct the deficiencies in their vulnerability reporting and tracking process to identify source machine/IP and plug-in IDs for critical vulnerabilities with their original report date versus relying upon the first report date identified in their vulnerability tracking report.

**PBGC Response:** PBGC concurs with this recommendation. ITIOD had already made improvements to its vulnerability tracking process in the months following the auditor's observations and has further plans, already in motion, to further improve vulnerability tracking and reporting.

**Target Completion Date: 6/30/2021**

**OIG Recommendation No. 2021-05-05: (NFR IT-2020-001)** PBGC should implement a modification to the PBGC access termination process to identify those separated employees and contractors who accessed their logical account or physically accessed PBGC facilities after their termination date. Further, once an instance has been identified PBGC should investigate this inappropriate access for reasonableness and capture details as a potential security incident.

**PBGC Response:** PBGC concurs with this recommendation. While PBGC has reliable procedures in place to block both logical and physical access to employees on their effective separation date/time, in the rare instances where a separation request is submitted after an employee or contractor has been terminated, PBGC will adjust its process to investigate any inappropriate access that may have occurred and if any is detected, open a security incident.

**Target Completion Date: 6/30/2021**

**OIG Recommendation No. 2021-05-06: (NFR IT-2020-007-FISMA-IAM)** PBGC should undertake efforts to train the user base on the level of detail required to gain access to CyberArk. Specifically, management should conduct a reasonable review of this activity against approved tickets or other documented, authorized procedures.

**PBGC Response:** PBGC concurs with this recommendation. ITIOD has efforts underway to ensure users receive the training necessary to properly document their use of CyberArk. ITIOD will also plan to conduct a reasonableness review of this activity against approved tickets or other documented, authorized procedures.

**Target Completion Date: 6/30/2021**

**OIG Recommendation No. 2021-05-07: (NFR IT-2020-008-FISMA-DPP)** 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 personally identifiable information (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.

**PBGC Response:** PBGC concurs with this recommendation. ITIOD will conduct an analysis to determine if the current PBGC internal network monitoring capabilities are sufficient to fully support PBGC's insider threat program, specifically around the monitoring of internal transmission of PII and sensitive banking information. Where appropriate, technically feasible, and practical to do so, we will deploy additional toolsets to monitor internal transmissions of PII and sensitive banking information for insider threat behavior analytic modeling.

**Target Completion Date: 6/30/2022**

**OIG Recommendation No. 2021-05-08: (NFR IT-2020-008-FISMA-DPP)** With the adoption of NIST 800-53 rev5, PBGC should conduct a risk assessment to consider the inclusion of the AU-13 optional control requirements for monitoring information disclosures by internal employees.

**PBGC Response:** PBGC concurs with this recommendation. ITIOD will assess the risk from information disclosure when migrating to 800-53 rev 5 and evaluate both baseline and supplementary controls related to information disclosure to address identified gaps with specific attention to AU-13.

**Target Completion Date: 6/30/2022**

**OIG Recommendation No. 2021-05-09: (NFR IT-2020-009-FISMA-DPP)** PBGC should conduct a Data Breach tabletop exercise, as well as monitor and analyze qualitative and quantitative performance measures on the effectiveness of its exercise.

**PBGC Response:** PBGC concurs with this recommendation. While a data breach tabletop was not conducted this fiscal year, this was due to unforeseen circumstances and is atypical of PBGC. We will continue to conduct tabletop exercises moving forward.

**Target Completion Date: 9/30/2021**

**OIG Recommendation No. 2021-05-10: (NFR IT-2020-010-FISMA-ST)** PBGC should utilize the Workforce Assessment Dashboard to determine how to fill gaps through the training or hiring of additional staff or contractors, as well as prepare an estimated timeline to fill this requirement.

**PBGC Response:** PBGC concurs with this recommendation. ECD has opened POA&M 3264 to establish a plan for addressing known gaps and new/existing and applicable work roles. ECD will collaborate with the Cybersecurity and Privacy Council to develop a Cybersecurity Work Role Plan for identifying critical Cyber functions aligned with the NIST NICE Framework (NIST SP 800-181).

**Target Completion Date: 6/30/2021**

**OIG Recommendation No. 2021-05-11: (NFR IT-2020-010-FISMA-ST)** PBGC should also share the gaps in the Workforce Assessment Dashboard with hiring managers so that they can understand the gaps and vet applicants who have the Knowledge, Skills, and Abilities (KSAs) to perform needed cybersecurity tasks.

**PBGC Response:** PBGC concurs with this recommendation**.** ECD has opened POA&M 3264 to establish a plan for addressing known gaps and new/existing and applicable work roles. ECD will collaborate with the Cybersecurity and Privacy Council to develop a Cybersecurity Work Role Plan for identifying critical Cyber functions aligned with the NIST NICE Framework (NIST SP 800-181) and share that information with hiring managers and various stakeholders to understand the gaps and vet applicants accordingly.

**Target Completion Date: 6/30/2021**

# Appendix D
# Additional Details Related to IT NFRs

## 4.4 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<br>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<br>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 and 2021-05-03 |
| NFR IT-2020-014 see | Inaccuracies with the first identified date in the report utilized by PBGC management in identifying vulnerabilities, led to open vulnerabilities not being tracked on the Patch and Vulnerability Management Group Tracker as required by PBGC policies. | NIST Special Publication 800-53, Revision 4<br>Control RA-05 Vulnerability Scanning | If management does not track and remediate open vulnerabilities, it increases the risk of leaving their environment vulnerable to unauthorized and fraudulent activity. | Recommendation Number 2021-05-04 |

| IT NFR Number | Cause | Criteria | Effect | Recommendation Number |
|---|---|---|---|---|
| NFR IT-2020-003-OIT-SOD | Management had not developed a cross-application role assignment for PBGC systems. Additionally, management had assigned one user roles that were incompatible per the SoD matrix. | NIST Special Publication 800-53, Revision 4<br>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 2021-02-08, 2021-02-09, 2021-02-10 and 2021-02-05 |
| NFR IT-2020-004-ONR-SOD<br>NFR IT-2020-011-OBA-SOD | Management did not completely and accurately document user roles conflicts within the Segregation of Duties matrices for information systems within the examination period. Where applicable, management did not adhere to the documented roles restrictions. | NIST Special Publication 800-53, Revision 4<br>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 2021-02-06, 2021-02-07, 2021-02-08, 2021-02-09 and 2021-02-10 |
| NFR IT-2020-005-FOD-SOD | Management did not completely and accurately document user roles conflicts within the Segregation of Duties matrices for information systems within the examination period. Where applicable, management did not adhere to the documented roles restrictions. | NIST Special Publication 800-53, Revision 4<br>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 2021-02-06, and 2021-02-08 |

| IT NFR Number | Cause | Criteria | Effect | Recommendation Number |
|---|---|---|---|---|
| NFR IT-2020-001_PBGC-Termination | Management did not follow the PBGC employee separation process. The delay in approval leads to the removal of logical access day(s) after the effective separation date. Further, management's process for monitoring the effectiveness of employee separations did not include a look-back review to determine if PBGC separations were executed in a timely manner. | NIST Special Publication 800-53, Revision 4<br>AC-2 Account Management | PBGC is exposed to the risk that separated employees will have unauthorized logical and physical access to information resources for fraud, waste or abuse. | Recommendation Number 2021-05-05 |
| NFR IT-2020-007-FISMA-IAM | During the FISMA performance audit, PBGC management stated that there is a requirement for users to enter a detailed justification to support the entry into CyberArk. However, the free-form nature of the justification field resulted in users inputting a high-level justification. | PBGC ITIOD Work Instruction: CyberArk User, Section 5: Brokering to a server or Device, Instruction 5.5.: "5.5 Type in a reason for connecting to the server, click OK"<br>NIST Special Publication 800-53, Revision 4<br>Control AU-3 Content of Audit Records | Without having a sufficient level of justification to support the need for entry into CyberArk, PBGC may not have visibility to determine why users are accessing the system, as well as lack transparency to effectively monitor whether access was justified. | Recommendation Number 2021-05-06 |

| IT NFR Number | Cause | Criteria | Effect | Recommendation Number |
|---|---|---|---|---|
| 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 |
| NFR IT-2020-009-FISMA-DPP | PBGC does have a documented Data Breach Response plan, however, no FY 2020 tabletop exercises were conducted. | NIST Special Publication 800-53, Revision 4<br>Control SE-2 Privacy Incident Response. | PBGC is exposed to the risk that their current Data Breach Response plan is not effectively understood by all parties, due to a lack of an exercise test and or/ lesson learned process. | Recommendation Number 2021-05-09 |

| IT NFR Number | Cause | Criteria | Effect | Recommendation Number |
|---|---|---|---|---|
| NFR IT-2020-010-FISMA-ST | PBGC management stated that they do track workforce gaps but have not yet identified a plan for addressing known gaps. | The Federal Cybersecurity Workforce Assessment Act of 2015 (Act) calls upon the Federal Government to conduct workforce planning for its cyber workforce.<br>NIST Special Publication (SP) 800-181<br>3.1 Identification of Cybersecurity Workforce Needs<br>3.2 Recruitment and Hiring of Highly Skilled Cybersecurity Talent | Gaps in the Workforce Assessment Dashboard could result in increased risk to PBGC, by creating holes in the identified roles requirements to maintain an adequate risk posture. | Recommendation Number 2021-05-10 and 2021-05-11 |

2011-3646362
ED None

**ey.com**