PBGC
Protecting America's Pensions

OFFICE OF INSPECTOR GENERAL
AUDIT REPORT

Pension Benefit Guaranty Corporation's Fiscal Year 2019 Compliance with the Federal Information Security Modernization Act of 2014

Report No. AUD-2020-5
December 20, 2019

Office of Inspector General

December 20, 2019

MEMORANDUM

TO: Gordon Hartogensis
Director

FROM: Brooke Holmes Brooke
Assistant Inspector General for Audits, Evaluations, and Inspections

SUBJECT: PBGC's Fiscal Year 2019 Federal Information Security Modernization Act Audit of 2014 (AUD-2020-5/FA-19-137-4)

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. CliftonLarsonAllen LLP, on behalf of the OIG, completed the OMB-required responses that we then submitted to OMB. This year, CliftonLarsonAllen LLP issued eight new FISMA-related recommendations. Two were issued in the Financial Statements audit report and six are issued in this report. PBGC agreed with the six new recommendations in this report and previously agreed with the two recommendations in the Financial Statements audit report.

We would like to take this opportunity to express our appreciation for the overall cooperation CliftonLarsonAllen 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's
Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2019

December 17, 2019

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

December 17, 2019

Robert A. Westbrooks
Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, NW
Washington, D.C. 20005-4026

Dear Mr. Westbrooks:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our performance audit of the Pension Benefit Guaranty Corporation's (PBGC) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) for fiscal year 2019.

We appreciate the assistance we received from PBGC and appreciate the opportunity to serve you. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Sincerely,

CliftonLarsonAllen LLP

S. Mirzakhani

Sarah Mirzakhani, CISA
Principal

CliftonLarsonAllen LLP
CLAconnect.com

Inspector General
Pension Benefit Guaranty Corporation

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the Pension Benefit Guaranty Corporation's (PBGC) information security program and practices for fiscal year 2019 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires agencies to develop, implement, and document an agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and report the results to the Office of the Management and Budget (OMB).

The objective of this performance audit was to determine the extent to which the PBGC's information security program and practices complied with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable OMB and National Institute of Standards and Technology (NIST) guidance.

Our audit was performed 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. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit included an assessment of PBGC's information security program and practices consistent with FISMA, and reporting instructions issued by OMB. The scope also included assessing select security controls outlined in NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of 5 of 22 systems in PBGC's FISMA inventory of information systems. We performed audit fieldwork at PBGC's headquarters in Washington, D.C., during the period April 2019 through November 2019.

There are five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1. According to the objective evaluation metrics of the Cybersecurity Framework, PBGC's security program, as in the prior year, fell below the specified threshold of effectiveness, *Managed and Measurable* (Level 4). PBGC's information security program achieved an overall *Consistently Implemented* (Level 3) maturity level. However, we did note areas of improvement in the Security Training and Information Security Continuous Monitoring domains – each moving up one level. In addition, two functional areas, *Detect* and *Respond*, were found to meet the *Managed and Measurable* (Level 4) maturity level.

We also concluded that PBGC's implementation of a subset of selected controls for selected information systems was not fully effective to ensure the confidentiality, integrity, and availability of the Corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, CLA noted weaknesses in 5 of the 8 Inspector General FISMA Metric Domains and have made a total of 8 new, and 20 repeated recommendations to assist PBGC in strengthening its information security program.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. We concluded our fieldwork and assessment on November 1, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 1, 2019.

The purpose of this audit report is to report on our assessment of PBGC's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Greenbelt, Maryland
December 17, 2019

Table of Contents

Executive Summary

The Pension Benefit Guaranty Corporation (PBGC or the Corporation) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA) requirement for an annual independent evaluation of PBGC's information security program. The objective of this performance audit was to determine the extent to which the PBGC's information security program and practices complied with FISMA requirements, Department of Homeland Security (DHS) reporting requirements, and applicable Office of Management Budget (OMB) and National Institute of Standards (NIST) guidance.

FISMA provides a comprehensive framework for ensuring effective security controls over information resources supporting federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The Act also provides a mechanism for improved oversight of federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program.

OMB and the DHS annually provide instructions to Federal agencies and Inspectors General (IGs) for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA Reporting Metrics[2] to independently assess their agencies' information security programs.

The FY 2019 IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. This assessment used objective metrics that are standardized across the federal government. To be considered effective, an agency's information security program must be rated at least *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5).

Audit Results

While PBGC continues to make progress in improving its information security and privacy program and its compliance with FISMA, OMB requirements, and applicable NIST guidance, its overall security program did not meet the requirements to be considered effective. According to the objective evaluation metrics of the IG FISMA Reporting Metrics, PBGC's security program fell

[1] FISMA (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] CLA submitted its responses to the FY 2019 IG FISMA Reporting Metrics to PBGC OIG as a separate deliverable.

below the specified threshold of effectiveness, *Managed and Measurable* (Level 4). PBGC's information security program achieved an overall *Consistently Implemented* (Level 3) maturity level. However, we did note areas of improvement in the Security Training and Information Security Continuous Monitoring domains – each moving up one level from the prior year. In addition, two functional areas, *Detect* and *Respond*, were found to meet the *Managed and Measurable* (Level 4) maturity level. Although, the Information Security Continuous Monitoring metric domain was rated as *Managed and Measurable*, we continue to identify areas of improvement needed for audit logging, audit monitoring and data loss prevention. **Table 1** shows a summary of the overall maturity levels for each domain in the FY 2019 IG FISMA Reporting Metrics.

Table 1: Maturity Levels for FY 2019 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions[3]	Metric Domains	Maturity
Identify	**Risk Management**	Consistently Implemented (Level 3)
Protect	**Configuration Management**	Consistently Implemented (Level 3)
	Identity and Access Management	Consistently Implemented (Level 3)
	Data Protection and Privacy	Consistently Implemented (Level 3)
	Security Training	Consistently Implemented (Level 3)
Detect	**Information Security Continuous Monitoring**	Managed and Measurable (Level 4)
Respond	**Incident Response**	Managed and Measurable (Level 4)
Recover	**Contingency Planning**	Consistently Implemented (Level 3)
Overall	**Consistently Implemented (Level 3)** **Not Effective**	

In addition, since last year, PBGC closed 6 out of 26 open recommendations reported in the FY 2018 FISMA audit[4] and continued to implement technologies and processes to address long standing access controls and configuration management weaknesses. PBGC realizes it requires cycle time and institutional maturity to fully resolve these security weaknesses. Continued focus is needed by PBGC management to effectively remediate the remaining risks and weaknesses in its information security program. Specifically, CLA noted weaknesses in risk management, vulnerability and configuration management, identity and access management, data protection and privacy, and information security continuous monitoring. **Table 2** below summarizes our detailed findings for FY 2019.

[3] See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

[4] See Appendix C for the status of prior year findings and recommendations.

Table 2: Cybersecurity Framework Security Functions Mapped to Weaknesses Noted in FY 2019 FISMA Audit

FY 2019 IG FISMA Metric Domains	Weaknesses Noted in FY 2019
Risk Management	Security documentation was not consistently reviewed, approved, updated and uploaded into the official and authoritative repository for system authorization and risk management.
	Security assessment and authorization documentation were not completed, or completed timely.
	Systems in ongoing authorization did not have the correct and up-to-date system security documentation recorded in the official tool.
	Plan of action and milestones were not established to mitigate risks identified in risk assessments.
	Lack of an insider threat detection and prevention program.
	Incomplete control implementation and assessment, and inadequate documentation of control inheritance[5] for the general support system.
	Interconnection Security Agreement between PBGC and the paying agent was not updated prior to expiration.
Configuration Management	Vulnerabilities were not tracked and remediated in a timely manner.
	Remediation of vulnerabilities identified in key databases and applications were not completed.
	Decommissioning of unsupported systems and databases were not completed.
	Lack of monitoring and noncompliance with web server baseline configuration.
Identity and Access Management	Untimely removal of terminated users' access by the effective separation date.
	Incomplete inactive account monitoring.
	Access to systems could not be verified.
	Inconsistent implementation of background investigation and re-investigation procedures.
Data Protection and Privacy	Some system technologies not upgraded or replaced to be compliant with encryption requirements.
	Project plans for data encryption has not been completed.
	Insufficient data loss prevention controls.
Information Security Continuous Monitoring	Critical auditable events have not been defined in security documents.
	Audit monitoring dashboards and reports are still in development.
	Insufficient data loss prevention controls.

[5] NIST SP 800-53, Revision 4, defines security control inheritance as "a situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides."

Overall, we conclude that information security at PBGC has improved in a number of areas. With continued effort, attention, and investment, the information security program will mature and can cross the effectiveness threshold in the near future. At the present time, however, the weaknesses noted leave PBGC operations and assets at risk of unauthorized access, misuse and disruption. To address these weaknesses, we made a total of 8 new, and 20 repeated recommendations to assist PBGC in strengthening its information security program.

The following section provides a detailed discussion of the audit findings grouped by the Cybersecurity Framework Security Functions. Appendix B describes the audit scope and methodology and Appendix C provides a status of prior year recommendations. In addition, PBGC management concurred with the recommendations and their comments are included in Appendix D.

FISMA Audit Findings

Security Function: Identify

Overview

PBGC developed and published the PBGC Risk Management Framework (RMF) process to fully implement its entity-wide information security risk management program. The RMF addresses both security and privacy controls. PBGC's IT risk management process focused on identifying and evaluating the threats and vulnerabilities to PBGC information. The RMF also focused on identifying risk management and mitigation strategies to address these threats and vulnerabilities. PBGC's risk management process was not fully effective since gaps and inconsistent implementation of the policies and procedures continue to exist.

Metric Domain – Risk Management

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk, organizations should understand the likelihood that an event will occur and the resulting impact. With this information, organizations can determine the acceptable level of risk for delivery of services and can express this as their risk tolerance. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* is guidance for implementing the risk management framework controls. The six step RMF includes security categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. The goal of the RMF is to provide near real-time risk management and ongoing authorization of information systems through robust continuous monitoring processes.

The following details the weaknesses noted in PBGC's risk management framework:

- PBGC officials did not properly maintain current security documentation within Cyber Security and Assessment Management (CSAM), PBGC's official and authoritative repository for system authorization and risk management. These security documents are required by PBGC policy to be uploaded to the CSAM system any time a change is made or a document is created. The security documents support the initial authorization, reauthorization, and ongoing authorization reviews of PBGC's systems.

  PBGC did not consistently review, approve, update, and upload required system security documentation in its CSAM repository tool for several of its systems. For example, there was security assessment and authorization documentation that was not completed, or completed timely, based on the Enterprise Cybersecurity Division's CSAM Quarterly Reviews for a selection of systems. Although the Security and Privacy Assessment and Authorization review identified documentation flaws, incomplete information, and missed reviews, the responsible parties were not correcting the identified items before expiration or need.

  There were documents that were not reviewed, approved, signed, and uploaded to the appropriate repository locations, in a timely manner. Specifically, the repository was not updated at the review frequencies listed within the RMF and in accordance with document review and update requirements. While Plan of Action and Milestones (POA&Ms) were created for the update, and review of actions required, the POA&Ms were not addressed in a timely manner.

- In FY 2019, PBGC completed a Risk Assessment for the Information Technology Infrastructure Services General Support System (ITISGSS). However, it was incomplete and plans of action and milestones were not established to mitigate identified risks. Upon notification of the issue, management provided a revised ITISGSS Risk Assessment Report; however, the new Risk Assessment Report was not included in the CSAM repository, as required.

- PBGC has not completed its implementation of an insider threat detection and prevention program. NIST SP 800-53, Rev. 4, security control PM-12, *Insider Threat Program*, indicates that the organization is required to implement an insider threat program that includes a cross-discipline insider threat incident handling team. In FY 2019, PBGC developed plans and established a timeline for implementing an insider threat program and plans to further refine the program in FY 2020.

- PBGC did not complete the implementation of NIST SP 800-53, Revision 4 controls that were designated as common controls,[6] remediate common controls weaknesses, and did not make the common controls available to system owners in CSAM for appropriate inclusion in their system security plans.

- The ITISGSS system owner did not complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4; did not revise its inheritance of common controls; nor conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4.

  The control assessment schedule for the general support system was not finalized and uploaded to CSAM until August 2019 for FY 2019. As a result, the general support system did not have an approved control assessment schedule from FY 2019 Quarter 1 to Quarter 3. Furthermore, after the official information security continuous monitoring (ISCM) plan was completed, a few controls were not assessed in accordance with the finalized plan.

- The Information Security Agreement between PBGC and a paying agent expired and was not renewed, or re-authorized prior or upon expiration. Due to a move of the PBGC Pension Lump Sum System (PLUS) data from an old vendor to a new one, the revisions of the agreement were delayed to ensure that the new boundary would be accurately reflected.

Without effective risk management controls, PBGC is at risk of controls not operating as intended or not being implemented, increasing the likelihood of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information.

[6] A common control is a security control that is inheritable by one or more organizational information systems.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Revise the processes and procedures of the continuous monitoring program to consistently enforce the review, update, and uploading of all required security assessment and authorization documentation for each system before the documentation expires. **(OIG Control Number FISMA-17-01)**

- Control owners should ensure the creation of plans of action and milestones, and risks within the Risk Assessment for all controls not fully implemented to mitigate risks. The appropriate control provider should be identified to correct/mitigate the identified weakness. **(OIG Control Number FISMA-18-04)**

- Office of Information Technology (OIT) should develop and implement procedures for the documentation of corrective actions within risk assessments. **(OIG Control Number FISMA-18-02)**

- OIT should update the Information Technology Infrastructure Services General Support System Risk Assessment to document corrective action plans. **(OIG Control Number FISMA-18-03)**

- PBGC should assign a senior organizational official, and develop and implement an insider threat detection and prevention program. **(OIG Control Number FISMA-16-14)**

- Complete the implementation of NIST SP 800-53, Revision 4 controls for common controls, remediation of common controls weaknesses and make available to system owners in Cyber Security Assessment and Management for appropriate inclusion in their system security plans. **(OIG Control Number FS-15-04)**

- Complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4; revise the inheritance of common controls; and conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4. **(OIG Control Number FISMA-17-02)**

- Maintain a valid agreement for all interconnections, and ensure that agreements are updated as necessary, reviewed annually, and re-issued prior to or upon expiration or upon a major change to ensure appropriate security and privacy controls are implemented. **(OIG Control Number FISMA-19-01)**

Security Function: Protect

Overview

PBGC continued to focus on resolving its access controls and configuration management weaknesses and continued to implement technologies and processes to address long standing control weaknesses. However, the controls require time to mature and show evidence of their operating effectiveness. In addition, management should continue to enhance processes by eliminating or reducing manual controls related to system access controls. PBGC realizes it requires cycle time and institutional maturity to fully resolve some security weaknesses. Weaknesses in the PBGC IT environment continue to contribute to deficiencies in system configurations, access controls, and data protection and privacy.

Metric Domain – Configuration Management

To secure both software and hardware, agencies must develop and implement standard configuration baselines that prevent or minimize exploitable system vulnerabilities. In addition, NIST has developed a repository of secure baselines for a wide variety of operating systems and devices.

CLA noted the following information security weaknesses in the Configuration Management domain:

- Although demonstrated improvements were made, vulnerabilities continue to exist and vulnerabilities were not remediated in a timely manner in accordance with organizational policies.

- PBGC has not completed the remediation of vulnerabilities identified in key databases and applications.

- We identified unsupported systems that were not tracked by PBGC for end of service life and plans for decommissioning of some unsupported systems and databases were not completed.

- PBGC did not monitor all web servers for compliance with baseline configuration standards. In addition, for the web servers that were monitored, we noted that they were not in compliance with baseline configurations.

We noted that the process and procedures for the tracking and remediation of individual vulnerabilities has been created. However, additional cycle time is required to confirm that the vulnerabilities are tracked and remediated within the timeframes established by PBGC policy.

The details related to PBGC's vulnerability management program, patch management, and configuration management weaknesses were noted in the issued FY 2019 Vulnerability Assessment and Penetration Test Report. The following technical recommendations were issued in the restricted report: OIT-158R, OIT-160R, OIT-161R, OIT-164R and OIT-167R.

Control weaknesses in the Configuration Management domain expose PBGC to increased risk of data compromise. Thus, PBGC may not have reasonable assurance that they are implementing sufficient processes to ensure the confidentiality, integrity and availability of information of its information systems.

Metric Domain – Identity and Access Management

Proper identity and access management ensures that users and devices are properly authorized to access information and information systems. Users and devices must be authenticated to ensure that they are who they identify themselves to be. In most systems, a username and password serve as the primary means of authentication, and the system enforces authorized access rules established by the system administrator. To ensure that only authorized users and devices have access to a system, policy and procedures must be in place for the creation, distribution, maintenance, and eventual termination of accounts. Homeland Security Presidential Directive 12 calls for all federal departments to require personnel to use personal identity verification cards. This use of personal identity verification cards is a major component of a secure, government-wide account and identify management system.

CLA noted the following information security weaknesses in the Identity and Access Management domain:

- We noted that PBGC has defined and improved processes for employee separations; however, the enhanced processes were recently implemented and we continued to identify discrepancies in the separation process for half of the fiscal year.

- There was a lapse in the reporting of inactive users of the paying agent's system due to the migration of data. As a result, a system generated listing of persons with inactive accounts to the PLUS application could not be produced and verified for appropriateness and need-to-know.

- Access to PBGC's data could not be verified for appropriateness and based on a need-to-know. Due to the paying agent's data migration, it resulted in PBGC's PLUS data stored on the paying agent's servers with other clients. Therefore, CLA was not able to audit the servers due to the conflict of other client data and information stored on the servers.

- PBGC did not consistently follow its background investigation process for new federal employees and contractors because the organization has not updated its policies and standard operating procedures.

- Enhancements to the background investigation process for existing personnel had not been completed at the time of audit fieldwork. PBGC is in process of testing compliance with the new procedures to ensure that background investigations are conducted for personnel that change positions and require a new background investigation for the new position's risk level, or have an expired background investigation and requires a re-investigation.

Control weaknesses in the Identity and Access Management domain expose PBGC to increased risk of data compromise. Thus, PBGC may not have reasonable assurance regarding the confidentiality and integrity of information in its systems.

Metric Domain – Data Protection and Privacy

FISMA requires the federal government to establish a privacy program and corresponding policies and procedures for the protection of personally identifiable information (PII) collected, used, maintained, shared, and disposed of by information systems. Training is to be provided for personnel responsible for PII or activities involving PII.

CLA noted the following information security weaknesses in the Data Protection and Privacy domain:

- PBGC is not fully compliant with the requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules* and OMB-A-130, *Managing Information as a Strategic Resource*. Specifically, PBGC has developed plans, to complete system technology upgrades or replacements to be compliant with FIPS 140-2 and OMB A-130; however, these plans are in various stages of planning or implementation. PBGC has accepted the risk for non-compliance. However, the acceptance of risk was not approved by the Chief Information Officer in accordance with OMB A-130.
- PBGC has not completed data encryption projects to address the recommendations made in their *PBGC IT Infrastructure Operations Department Risk Based Encryption Assessment*.

In addition, the details related to PBGC's vulnerability management program, and data loss prevention weaknesses were noted in the issued FY 2019 Vulnerability Assessment and Penetration Test Report. The following technical recommendations were issued in the restricted report: OIT-167R.

Control weaknesses in the Data Protection and Privacy domain expose PBGC to increased risk of compromise of data confidentiality for millions of participants.

Metric Domain – Security Training

FISMA requires all federal government personnel and contractors to complete annual security awareness training that provides instructions on threats to data security and responsibilities in information protection. FISMA also requires specialized training for personnel and contractors with significant security responsibilities. Without adequate security training programs, agencies cannot ensure that personnel would have the knowledge required to ensure the security of the information systems and data.

We did not find weaknesses in PBGC's Security Training Program.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- Develop and implement plans of action for addressing known security weaknesses. **(OIG Control Number FISMA FS-16-08)**

- Document and implement enhanced processes and procedures to effectively track and remediate known vulnerabilities in a timely manner. **(OIG Control Number FISMA-17-03)**

- Implement controls to remedy vulnerabilities identified in key databases and applications, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access. **(OIG Control Number FISMA FS-07-14)**

- Fully implement controls to plan, remove and decommission unsupported systems, software, and databases. **(OIG Control Number FISMA FS-16-07)**

- PBGC should implement effective processes and procedures to ensure the secure configuration of web servers in accordance with the established configuration baselines and document deviations to the established baselines on an as needed basis. **(OIG Control Number FISMA-17-04)**

- Implement improved processes and provide training to ensure PBGC federal managers/Contracting Officer Representatives submit and approve separation requests prior (when applicable) to the effective separation date, as well as the collection of IT Assets by the effective separation date. **(OIG Control Number FS-18-12)**

- Implement improved processes and provide training to ensure PBGC Workplace Solutions Department removes physical access by the effective separation date. **(OIG Control Number FS-18-13)**

- Office of Benefits Administration should document enhanced account management procedures to ensure a thorough review of accounts is performed during the annual account recertification and that necessary accounts are recertified, and implement compensating controls to verify inactive accounts are deactivated in accordance with PBGC policy. **(OIG Control Number FS-17-05)**

- OBA should obtain confirmation of access to server or in the event the access list cannot be shared, PBGC will pursue viable alternatives to include moving PBGC data to a separate server within the paying agent's data center. (**OIG Control Number FS-19-10)**

- Conduct an account recertification of Linux users and groups with access to PBGC PLUS data to verify that only authorized users have access and the privileges are appropriate. **(OIG Control Number FS-19-11)**

- Improve processes and implement oversight to ensure timeliness of background investigations to be completed for federal employees and contractors. **(OIG Control Number FISMA-19-02)**

- Update directives, policies, and procedures to reflect current personnel security processes for the timely processing of background investigations. **(OIG Control Number FISMA-19-03)**

- 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. **(OIG Control Number FISMA-14-15)**

- Develop and implement plans for completing system technology upgrades or replacements to be compliant with FIPS 140-2 and OMB A-130. **(OIG Control Number FS-18-09)**

- Develop and implement project plans for satisfying the recommendations that were made in the *PBGC IT Infrastructure Operations Department Risk Based Encryption Assessment*, dated June 29, 2018, version 1.0. **(OIG Control Number FS-18-10)**

Security Function: Detect

Overview

In FY 2019 PBGC continued to enhance implementation of various tools and processes to detect threats and vulnerabilities to improve its continuous monitoring program. With the continued maturity and deeper implementation of these tools and processes, PBGC's continuous monitoring program is becoming more effective.

Metric Domain – Information Security Continuous Monitoring

The goal of Information Security Continuous Monitoring is to combat information security threats by maintaining ongoing awareness of information security, vulnerabilities, and threats to federal systems and information. Information Security Continuous Monitoring provides ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity posture, hygiene, and operational readiness.

CLA noted the following information security weaknesses in the Information Security Continuous Monitoring domain:

- Critical auditable events have been defined by system owners. However, security documentation, including the system security plans, have not yet been updated to identify the critical auditable events. In addition, PBGC has not completed the development of Splunk[7] dashboards and reports of some critical auditable events for application owners.

- PBGC has completed an assessment of their data loss prevention program to identify gaps in their toolsets. However, the gaps identified in the assessment have not yet been remediated.

Control weaknesses in the Information Security Continuous Monitoring domain continue to expose PBGC to threats and vulnerabilities that could bypass its defenses, which may result in compromise and increased risk of unauthorized modification, loss, and disclosure of critical and sensitive PBGC information. Thus, PBGC may not have reasonable assurance regarding the confidentiality, integrity, and availability of information in its systems.

Recommendations:

We recommend that PBGC improve the security of its environment by doing the following:

- System Owners should conduct and document an analysis of major applications' critical auditable events and business transactions to identify audit logging needs and requirements. **(OIG Control Number FISMA-15-02)**

- System Owners should develop and implement plans to fully implement Splunk Enterprise for their major applications. **(OIG Control Number FS-07-17)**

[7] Splunk is PBGC's Security Information and Event Management (SIEM) tool. Splunk allows for the aggregation of various system and applications logs to allow for real-time event monitoring and analysis.

- Enhance and improve PBGC's Data Loss Prevention (DLP) policies and procedures for PBGC personnel and DLP toolset as identified in the *Data Loss Prevention Controls Adequacy Assessment*, version 1.0, dated June 29, 2017. **(OIG Control Number FISMA-19-04)**

- Complete the identification and documentation of the location of sensitive data in all environments (at the host-level) and attendant data flows. **(OIG Control Number FISMA-19-05)**

- Enhance and improve PBGC's technological capability to detect and block personally identifiable information (PII) transferred using encrypted protocols (e.g. SFTP or HTTPS). **(OIG Control Number FISMA-19-06)**

Security Function: Respond

Overview

In FY 2019, PBGC met its established timelines for responding to security incidents and followed its processes and procedures for handling incidents.

Metric Domain – Incident Response

Information security incidents occur on a daily basis. Agencies must have sound policies and planning in place to respond to these incidents and report them to the appropriate authorities. The United States Computer Emergency Readiness Team is to receive reports of incidents on unclassified Federal Government systems, and OMB requires the reporting of incidents that involve sensitive data, such as personally identifiable information, within strict timelines.

We did not find weaknesses in PBGC's Incident Response program.

Recommendations:

None.

Security Function: Recover

Overview

PBGC has an established process and an annual program for testing and documenting lessons learned from the annual test exercise.

Metric Domain – Contingency Planning

FISMA requires agencies to prepare for events that may affect an information resource's availability. This preparation requires identification of resources and risks to those resources, and the development of a plan to address the consequences if loss of a system's availability occurs. Consideration of risk to an agency's mission and the possible magnitude of harm caused by a resource's unavailability are key to contingency planning. NIST SP 800-34, Revision 1*,* *Contingency Planning Guide for Federal Information Systems*, defines contingency planning as "interim measures to recover information system services after a disruption. Interim measures may include relocation of information systems and operations to an alternate site, recovery of information system functions using alternate equipment, or performance of information system functions using manual methods." Once a contingency plan is established, training and testing must be conducted to ensure that the plan and individuals tasked with the contingency responsibilities will be capable in the event of an emergency.

PBGC has consistently implemented contingency planning processes but has not reached a level of maturity as defined by the IG FISMA Reporting Metrics to be an effective overall program.[8] This is mainly because PBGC's contingency plan program has not addressed supply chain risks posed to its contingency plan program. In addition, PBGC does not collect metrics on the effectiveness of its information system contingency plans and 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 PBGC. Although PBGC maturity was not effective in the Contingency Planning domain, we did not find weaknesses in PBGC's Contingency Planning program.

Recommendations:

None.

[8] A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

Appendix A: Background

Overview

PBGC protects the pensions of nearly 37 million workers and retirees in more than 25,000 plans. Under Title IV of the Employee Retirement Income Security Act of 1974, PBGC insures, subject to statutory limits, pension benefits of participants in covered private defined-benefit pension plans in the United States. To accomplish its mission, PBGC relies extensively on the effective operation of information technology controls. As a result, the reliability of computerized data and of the systems that process, maintain, and report this data are major priorities for PBGC. Although the increase in computer interconnectivity has changed the way the government does business, it has also increased the risk of loss and misuse of information by unauthorized or malicious users. Protecting information systems continues to be one of the most important challenges facing government organizations today.

Federal Information Security Modernization Act of 2014

FISMA requires agencies to develop, document, and implement agency-wide programs to provide information security for the information and information systems that support their operations and assets and requires the agencies' Inspector General to test the security of a representative subset of the agency's systems and assess the effectiveness of information security policies, procedures, and practices of the agency.

In addition, FISMA requires agencies to implement the following:

- Periodic risk assessments.
- Information security policies, procedures, standards, and guidelines.
- Delegation of authority to the Chief Information Officer (CIO) to ensure compliance with policy.
- Security awareness training programs.
- Periodic (annual and more frequent) testing and evaluation of the effectiveness of security policies, procedures, and practices.
- Processes to manage remedial actions for addressing deficiencies.
- Procedures for detecting, reporting, and responding to security incidents.
- Plans to ensure continuity of operations.
- Annual reporting on the adequacy and effectiveness of its Information Security Program.

FY 2019 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. Accordingly, the FY 2019 IG FISMA Reporting Metrics provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[9]

[9] Available online at https://www.dhs.gov/publication/fy19-fisma-documents.

The FY 2019 IG FISMA Reporting Metrics are structured around the five information security functions outlined in NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 3**.

Table 3: Aligning the Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 4** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*.

Table 4: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Appendix B: Scope and Methodology

Scope

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

The objective of this audit was to determine the extent to which PBGC's information security program and practices complied with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance.

The scope of this performance audit was to assess PBGC's information security program consistent with FISMA, and reporting instructions issued by OMB and DHS. CLA performed a vulnerability assessment and penetration testing and assessed selected security controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the following sample of five systems from the 22 systems in PBGC's FISMA inventory of information systems:

- Consolidated Financial System
- Trust Accounting System
- Pension Lump Sum Program
- Information Technology Infrastructure Services General Support System
- Integrated Present Value of Future Benefits

In addition, the audit included an assessment of effectiveness for each of the eight FY 2019 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions.

The audit also included a follow up on prior audit recommendations to determine if PBGC made progress in implementing the recommended improvements concerning its information security program.

Audit fieldwork was performed at PBGC's headquarters in Washington, DC, during the period April 2019 through November 2019.

Methodology

To accomplish the audit objective, CLA:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to PBGC's information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, and continuous monitoring plan.

- Tested system processes to determine the adequacy and effectiveness of selected controls.
- Reviewed the status of recommendations in the prior year FISMA report, including supporting documentation to ascertain whether the actions taken addressed the weaknesses.

In addition, CLA assessed PBGC's technical controls by performing a network security test as part of the FISMA audit. The independent vulnerability assessment and penetration test was conducted to determine the effectiveness of internal controls that prevent and detect unauthorized access, disclosure, modification, or deletion of sensitive information. The results of the vulnerability assessment and penetration test was incorporated into our FISMA audit results.

To perform our review of PBGC's security program, we followed a work plan based on the following guidance:

- OMB and DHS, FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics.
- NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.
- NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*.
- NIST SP 800-53A*,* Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).
- Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM: GAO-09-232G), for the information technology audit methodology.

In testing for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. In some cases, this resulted in selecting the entire population. However, in cases where an entire audit population was not selected, the results cannot be projected and if projected may be misleading.

Appendix C: Status of Prior Year Recommendations

The following is the status of prior year recommendations.

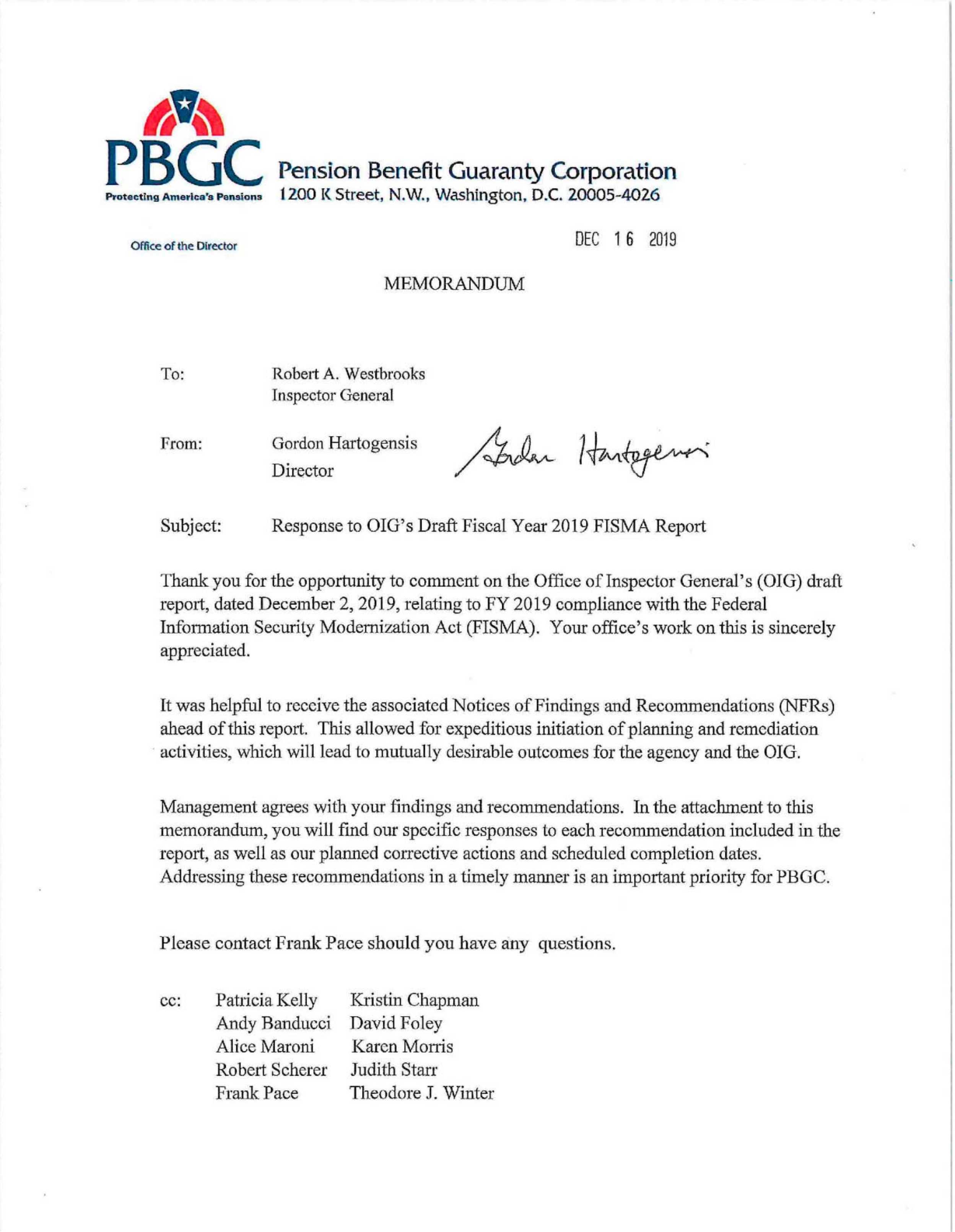
FISMA Recommendations Closed in Fiscal Year 2019

OIG Control Number	Date Closed	Original Report Number
FS-14-12	November 7, 2019	AUD-2015-3/FA-14-101-3
FS-18-11	September 23, 2019	AUD-2019-1/FA-18-127-1
FISMA-15-01	October 31, 2019	EVAL-2016-7/FA-15-108-7
FISMA-15-05	November 8, 2019	EVAL-2016-7/FA-15-108-7
FISMA-18-01	October 3, 2019	AUD-2019-04/FA-18-127-4
FISMA-18-05	November 22, 2019	AUD-2019-04/FA-18-127-4

Prior and Current Years' Open FISMA Recommendations in Fiscal Year 2019

OIG Control Number	Original Report Number
Prior Year	
FS-07-14	2008-2/FA-0034-2
FS-07-17	2008-2/FA-0034-2
FS-15-04	AUD-2016-3/FA-15-108-3
FS-16-07	AUD-2017-3/FA-16-110-2
FS-16-08	AUD-2017-3/FA-16-110-2
FS-17-05	AUD-2018-6/FA-17-19-3
FS-18-09	AUD-2019-1/FA-18-127-1
FS-18-10	AUD-2019-1/FA-18-127-1
FS-18-12	AUD-2019-1/FA-18-127-1
FS-18-13	AUD-2019-1/FA-18-127-1
FISMA-14-15	EVAL-2015-9/FA-14-101-7
FISMA-15-02	EVAL-2016-7/FA-15-108-7
FISMA-16-14	EVAL-2017-9 /FA-16-110-7
FISMA-17-01	EVAL-2018-7/FA-17-119-6
FISMA-17-02	EVAL-2018-7/FA-17-119-6
FISMA-17-03	EVAL-2018-7/FA-17-119-6
FISMA-17-04	EVAL-2018-7/FA-17-119-6
FISMA-18-02	AUD-2019-04/FA-18-127-4
FISMA-18-03	AUD-2019-04/FA-18-127-4
FISMA-18-04	AUD-2019-04/FA-18-127-4
Current Year	
FISMA-19-01	
FISMA-19-02	
FISMA-19-03	
FISMA-19-04	
FISMA-19-05	
FISMA-19-06	
FS-19-10	AUD-2020-2/FA-19-137-1
FS-19-11	AUD-2020-2/FA-19-137-1

Appendix D: Management Comments



PBGC
Protecting America's Pensions

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

Office of the Director

DEC 16 2019

MEMORANDUM

To: Robert A. Westbrooks
Inspector General

From: Gordon Hartogensis
Director

Gordon Hartogensis

Subject: Response to OIG's Draft Fiscal Year 2019 FISMA Report

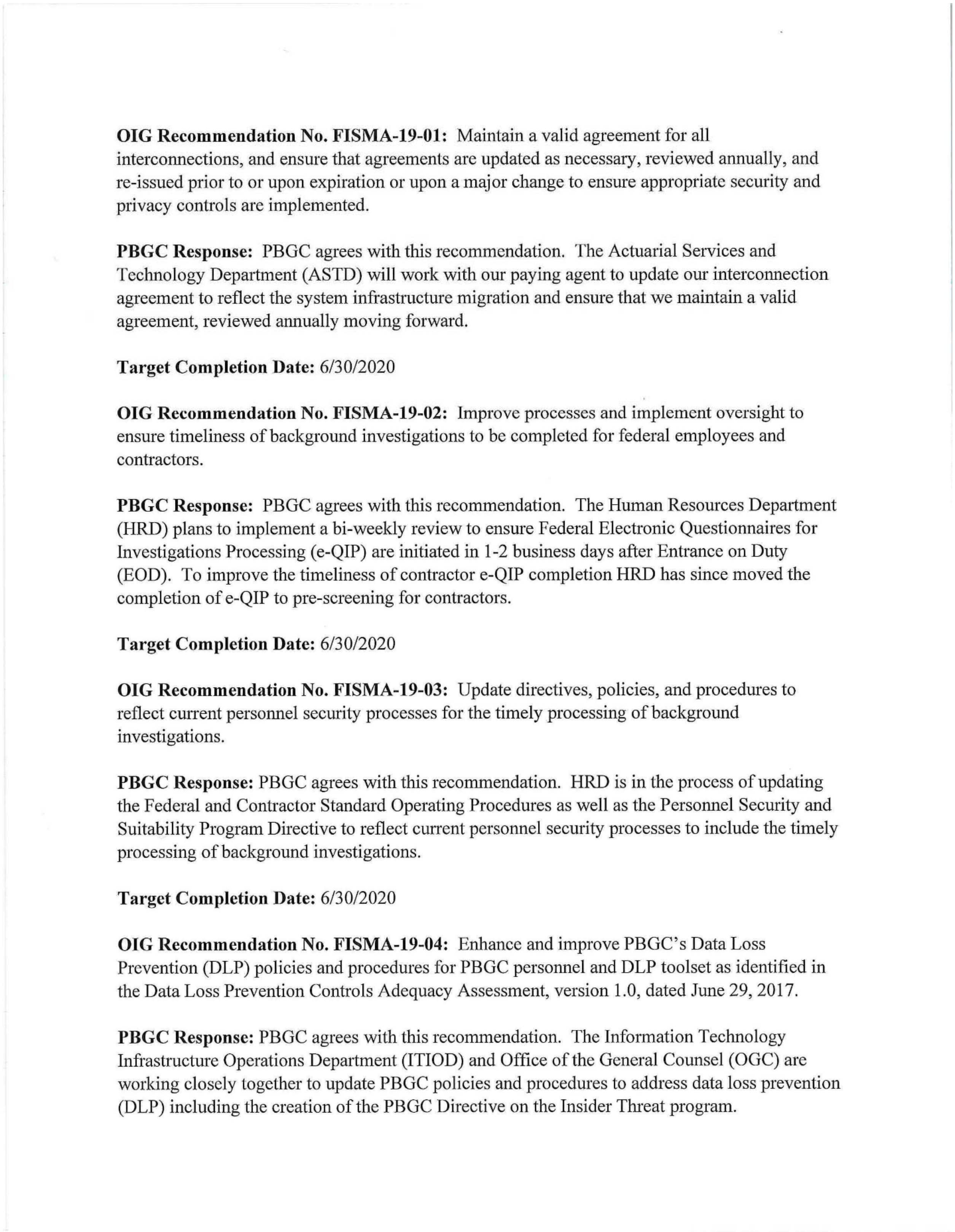
Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, dated December 2, 2019, relating to FY 2019 compliance with the Federal Information Security Modernization Act (FISMA). Your office's work on this is sincerely appreciated.

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 recommendation included in the report, as well as our planned corrective actions and scheduled completion dates. Addressing these recommendations in a timely manner is an important priority for PBGC.

Please contact Frank Pace should you have any questions.

cc:
Patricia Kelly
Andy Banducci
Alice Maroni
Robert Scherer
Frank Pace
Kristin Chapman
David Foley
Karen Morris
Judith Starr
Theodore J. Winter



OIG Recommendation No. FISMA-19-01: Maintain a valid agreement for all interconnections, and ensure that agreements are updated as necessary, reviewed annually, and re-issued prior to or upon expiration or upon a major change to ensure appropriate security and privacy controls are implemented.

PBGC Response: PBGC agrees with this recommendation. The Actuarial Services and Technology Department (ASTD) will work with our paying agent to update our interconnection agreement to reflect the system infrastructure migration and ensure that we maintain a valid agreement, reviewed annually moving forward.

Target Completion Date: 6/30/2020

OIG Recommendation No. FISMA-19-02: Improve processes and implement oversight to ensure timeliness of background investigations to be completed for federal employees and contractors.

PBGC Response: PBGC agrees with this recommendation. The Human Resources Department (HRD) plans to implement a bi-weekly review to ensure Federal Electronic Questionnaires for Investigations Processing (e-QIP) are initiated in 1-2 business days after Entrance on Duty (EOD). To improve the timeliness of contractor e-QIP completion HRD has since moved the completion of e-QIP to pre-screening for contractors.

Target Completion Date: 6/30/2020

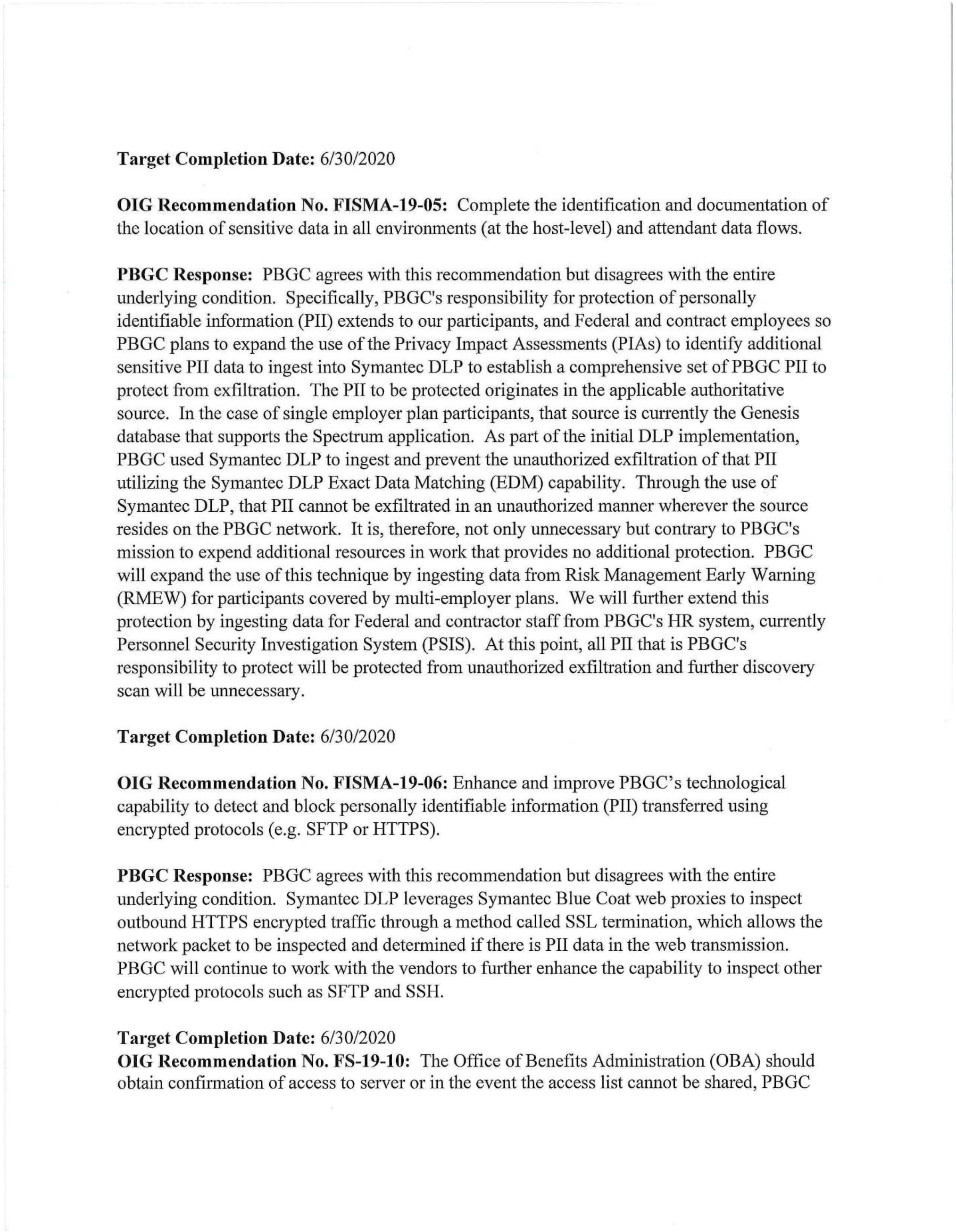
OIG Recommendation No. FISMA-19-03: Update directives, policies, and procedures to reflect current personnel security processes for the timely processing of background investigations.

PBGC Response: PBGC agrees with this recommendation. HRD is in the process of updating the Federal and Contractor Standard Operating Procedures as well as the Personnel Security and Suitability Program Directive to reflect current personnel security processes to include the timely processing of background investigations.

Target Completion Date: 6/30/2020

OIG Recommendation No. FISMA-19-04: Enhance and improve PBGC's Data Loss Prevention (DLP) policies and procedures for PBGC personnel and DLP toolset as identified in the Data Loss Prevention Controls Adequacy Assessment, version 1.0, dated June 29, 2017.

PBGC Response: PBGC agrees with this recommendation. The Information Technology Infrastructure Operations Department (ITIOD) and Office of the General Counsel (OGC) are working closely together to update PBGC policies and procedures to address data loss prevention (DLP) including the creation of the PBGC Directive on the Insider Threat program.



Target Completion Date: 6/30/2020

OIG Recommendation No. FISMA-19-05: Complete the identification and documentation of the location of sensitive data in all environments (at the host-level) and attendant data flows.

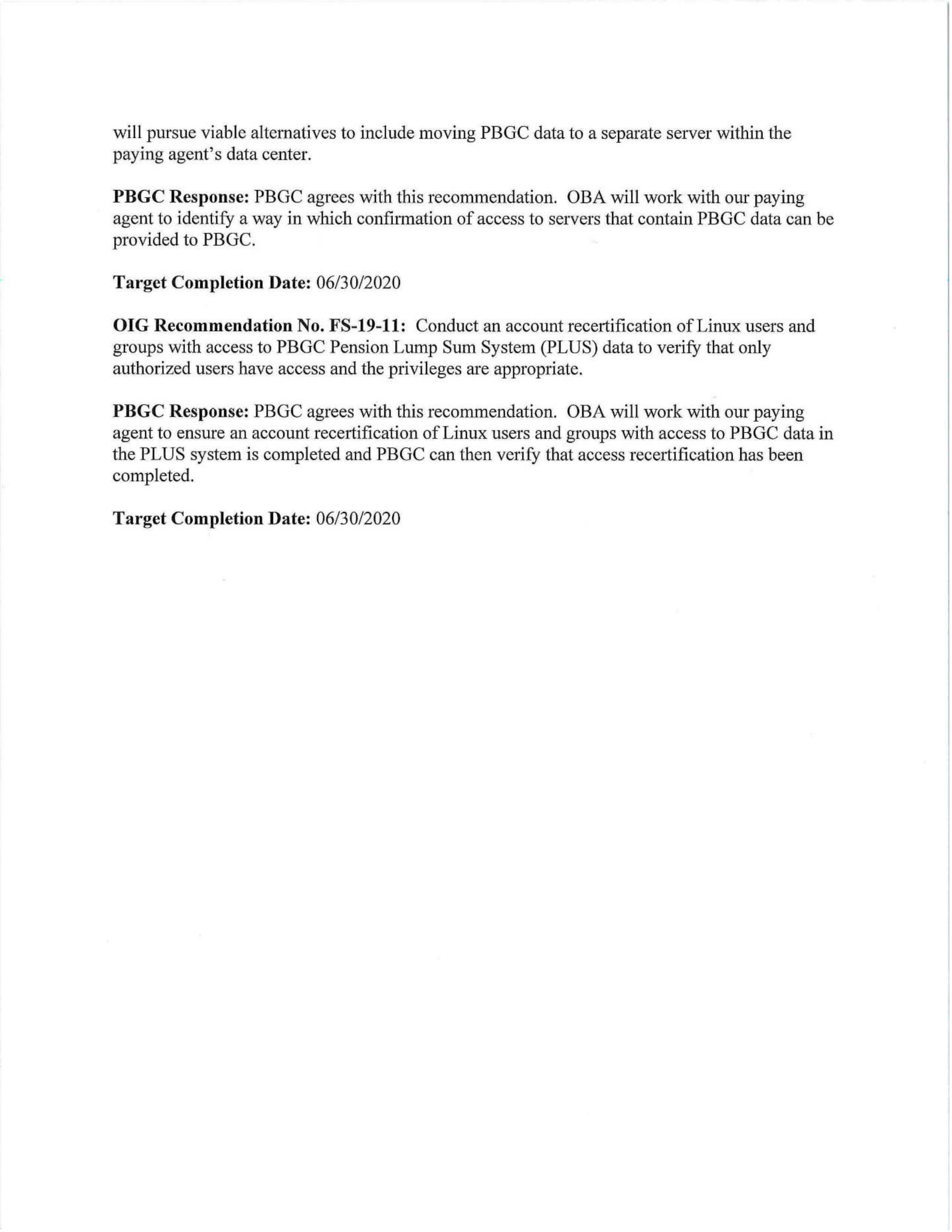
PBGC Response: PBGC agrees with this recommendation but disagrees with the entire underlying condition. Specifically, PBGC's responsibility for protection of personally identifiable information (PII) extends to our participants, and Federal and contract employees so PBGC plans to expand the use of the Privacy Impact Assessments (PIAs) to identify additional sensitive PII data to ingest into Symantec DLP to establish a comprehensive set of PBGC PII to protect from exfiltration. The PII to be protected originates in the applicable authoritative source. In the case of single employer plan participants, that source is currently the Genesis database that supports the Spectrum application. As part of the initial DLP implementation, PBGC used Symantec DLP to ingest and prevent the unauthorized exfiltration of that PII utilizing the Symantec DLP Exact Data Matching (EDM) capability. Through the use of Symantec DLP, that PII cannot be exfiltrated in an unauthorized manner wherever the source resides on the PBGC network. It is, therefore, not only unnecessary but contrary to PBGC's mission to expend additional resources in work that provides no additional protection. PBGC will expand the use of this technique by ingesting data from Risk Management Early Warning (RMEW) for participants covered by multi-employer plans. We will further extend this protection by ingesting data for Federal and contractor staff from PBGC's HR system, currently Personnel Security Investigation System (PSIS). At this point, all PII that is PBGC's responsibility to protect will be protected from unauthorized exfiltration and further discovery scan will be unnecessary.

Target Completion Date: 6/30/2020

OIG Recommendation No. FISMA-19-06: Enhance and improve PBGC's technological capability to detect and block personally identifiable information (PII) transferred using encrypted protocols (e.g. SFTP or HTTPS).

PBGC Response: PBGC agrees with this recommendation but disagrees with the entire underlying condition. Symantec DLP leverages Symantec Blue Coat web proxies to inspect outbound HTTPS encrypted traffic through a method called SSL termination, which allows the network packet to be inspected and determined if there is PII data in the web transmission. PBGC will continue to work with the vendors to further enhance the capability to inspect other encrypted protocols such as SFTP and SSH.

Target Completion Date: 6/30/2020
OIG Recommendation No. FS-19-10: The Office of Benefits Administration (OBA) should obtain confirmation of access to server or in the event the access list cannot be shared, PBGC



will pursue viable alternatives to include moving PBGC data to a separate server within the paying agent's data center.

PBGC Response: PBGC agrees with this recommendation. OBA will work with our paying agent to identify a way in which confirmation of access to servers that contain PBGC data can be provided to PBGC.

Target Completion Date: 06/30/2020

OIG Recommendation No. FS-19-11: Conduct an account recertification of Linux users and groups with access to PBGC Pension Lump Sum System (PLUS) data to verify that only authorized users have access and the privileges are appropriate.

PBGC Response: PBGC agrees with this recommendation. OBA will work with our paying agent to ensure an account recertification of Linux users and groups with access to PBGC data in the PLUS system is completed and PBGC can then verify that access recertification has been completed.

Target Completion Date: 06/30/2020