




Office of Inspector General  
Pension Benefit Guaranty Corporation

August 11, 2016

Sensitive information about the Pension Benefit Guaranty Corporation's information technology infrastructure has been redacted.

**TO:** Robert P. Scherer, Chief Information Officer  
Pension Benefit Guaranty Corporation

**FROM:** Nina Murphy   
Assistant Inspector General for Audits, Evaluations and  
Reviews

**SUBJECT:** FY 2015 Cybersecurity Act Evaluation (EVAL-2016-10/IT-16-111)

In accordance with Section 406 of the Cybersecurity Act of 2015, we evaluated aspects of PBGC computer systems that provide access to personally identifiable information (PII).<sup>1</sup> Our objective was to provide descriptions of certain policies, practices, and procedures identified in the statute and listed below. The scope of our work was limited to obtaining and analyzing PBGC's information security policies, practices, and procedures governing computer systems that provide access to PII. We did not test the Corporation's internal controls or compliance with the policies and procedures provided in this report. Information on whether the Corporation followed the appropriate standards was based on OIG open recommendations and the Corporation's Plan of Actions and Milestones.

---

<sup>1</sup> In accordance with National Institute of Standards and Technology Special Publication 800-122, PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

## Background

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. PBGC protects the pensions of more than 41 million U.S. workers and retirees in more than 24,000 plans. To accomplish its mission and prepare its financial statements, PBGC relies extensively on the effective operation of information systems. Internal controls are essential to ensure the confidentiality, integrity, and availability of critical data, while reducing the risk of errors, fraud, and other illegal acts. While 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. As evidenced by recent large-scale attacks on federal information systems and data at various agencies, including the Office of Personnel Management, cybersecurity threats continue to present significant challenges.

The Federal Information Security Management Act (FISMA) of 2002 established the requirement for federal agencies to develop, implement and manage agency-wide information security programs. Federal agencies are also required to provide acceptable levels of security for the information and systems that support their operations and assets. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 was developed to further agency statutory responsibilities under FISMA. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.

To address cybersecurity threats, in December 2015, President Obama signed into law the Cybersecurity Act of 2015. Section 406—Federal Computer Security—requires that no later than 240 days after enactment of this act (by August 14, 2016), the Inspector General of each covered agency<sup>2</sup> submit reports to Congress on information collected from the covered agency on national security systems and/or federal computer systems that provide access to PII. The act requires that the report contain the following:

- A. A description of the logical access policies and practices used by the covered agency to access a covered system,<sup>3</sup> including whether appropriate standards were followed.
- B. A description and list of the logical access controls and multi-factor authentication used by the covered agency to govern access to covered systems by privileged users.

---

<sup>2</sup> As defined in the Cybersecurity Act of 2015, the term “covered agency” means an agency that operates a covered system.

<sup>3</sup> The Cybersecurity Act of 2015 designated “covered system” as any federal computer system that provides access to PII.

- C. If the covered agency does not use logical access controls or multi-factor authentication to access a covered system, a description of the reasons for not using such logical access controls or multi-factor authentication.
- D. A description of the following information security management practices used by the covered agency regarding covered systems:
- (i) The policies and procedures followed to conduct inventories of the software present on the covered systems of the covered agency and the licenses associated with such software.
  - (ii) What capabilities the covered agency utilizes to monitor and detect exfiltration and other threats, including:
    - a. data loss prevention capabilities;
    - b. forensics and visibility capabilities; or
    - c. digital rights management capabilities.
  - (iii) A description of how the covered agency is using the capabilities described in clause (ii).
  - (iv) If the covered agency is not utilizing capabilities described in clause (ii), a description of the reasons for not utilizing such capabilities.
- E. A description of the policies and procedures of the covered agency with respect to ensuring that entities, including contractors, that provide services to the covered agency are implementing the information security management practices described in subparagraph (D).

## **PBGC's Covered Systems**

PBGC depends on computerized information systems to execute its operations and to process, maintain and report essential information. Of the 18 FISMA reportable systems, 15 provide access to PII that could include information relating to individual participants and beneficiaries in covered pension plans, or individual PBGC employees or contractors.

The following systems contain PII and are managed by PBGC:

- Administar (ADM)
- BAPD Application Suite (BAS)
- Consolidate Financial System (CFS)
- Corporate Performance System (CPS)
- Facilities Services Program (FSP)
- IT Infrastructure Services General Support System (ITSGSS)
- Legacy Record Search/Retrieval System (LRSRS)

- Legal Technologies Program (LTP)
- My Plan Administration Account (My PAA)
- Procurement Management Program (PMP)
- Risk Management Early Warning (RMEW)

The following systems contain PII and are managed by contractors:

- The Pension Lump Sum Program (PLUS)
- Electronic Complaint and Tracking System (eCATS)
- eDiscovery
- Human Resource Management System (HRMS)

## **A . A description of the logical access policies and practices**

NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, provides a catalog of security and privacy controls for federal information systems and a process for selecting controls. The controls in NIST SP 800-53 are organized in 18 security control families including Access Controls (AC) and Identification and Authentication (IA) controls. A subset of the controls in these two families guides PBGC processes for granting and denying requests to obtain and use information and related information processing services. PBGC has not fully migrated to NIST SP 800-53, Revision 4; therefore, some applicable NIST SP 800-53 controls are based on Revision 3.

Access Control Policy and Procedures (AC-1) and Identification and Authentication Policy and Procedures (IA-1) standards of NIST SP 800-53 address, respectively, the establishment of policies and procedures for the effective implementation of selected security controls and control enhancements in the AC and IA families. PBGC addresses logical access to covered systems through a combination of Information Security Policy, Information Security Standards and OIT standard operating procedures. PBGC Directive IM-05-02 established the PBGC Information Security Policy and outlined PBGC security policy for meeting NIST SP 800-53 guidance. The security policies set forth in the Directive IM-05-02 must be followed by all PBGC's information systems (regardless of location or delivery mechanism) in order to ensure confidentiality, integrity and availability of data in PBGC information systems.

Directive IM-05-02 established policies that are derived from, and embodied by, the PBGC Information Security Standards and Information Security Controls Matrix. The policies set forth



in the Directive are supported by OIT standards, processes, procedures and guidelines and reviewed and approved by the OIT Governance Boards.<sup>4</sup>

The policies are classified into four security control categories: management, operational, technical, and program management. Technical controls included in this directive are implemented and executed primarily in an automated fashion and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system and require the following controls in AC and IA families:

- Information systems employ methods to identify and authenticate users, devices and processes (AC control family).
- Access be granted to, and removed from, users and/or user groups as appropriate (AC control family).
- Controls appropriate to the mode of connection (e.g., wireless, remote, etc.) shall be in place on information systems (AC control family).
- Users, processes, and devices shall be properly identified and authenticated before being connected to system resources (IA control family).

### ***Standards***

PBGC's Information Security Standards are technical standards that apply to all information systems used and operated by PBGC, a contractor of PBGC or another organization on behalf of PBGC. These standards address NIST SP 800-53 requirements of AC and IA control families.

PBGC issued the Identity, Credential, and Access Management (ICAM) interim standard to enable the adoption of more consistent, efficient and effective services across PBGC in the near term, and to ensure compliance with federal mandates, guidance and best practices. The ICAM interim standard is a resource for PBGC implementers and consumers of identity, credential and access management services. The ICAM interim standards are comprised of the programs, processes, technologies and personnel used to create trusted digital identity representations of individuals and Non-Person Entities (NPEs). They bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions and leverages the credentials to provide authorized access to the Corporation's resources. They apply to all IT solutions

---

<sup>4</sup> Based on PBGC Directive IM-05-02, the OIT Governance Boards are formal groups chartered to ensure that all OIT policies, processes, standards and procedures are developed, coordinated and implemented using an integrated approach; are compliant with federal and PBGC policies; are auditable; and are reviewed for continuous improvement.

development teams and the primary stakeholders and actors participating in development activities that need to understand the target ICAM architecture. See Appendix 2.

### ***Standard Operating Procedures***

PBGC's OIT standard operating procedures (SOPs) describe the procedures when a federal employee or contractor requests a new user account; is removed from service; is transferred to another position, division, and/or department within the Corporation; and when a federal employee's or contractor's logical and workspace access or assets are modified. Each of these SOPs addresses purpose, scope, roles, responsibilities, quality controls and key performance indicators. These SOPs partially or fully address NIST SP 800-53 controls of AC and IA families. See Appendix 3.

### ***Other Process***

PBGC requires annual recertification of user accounts to access information systems, business applications and the data stored or processed by these systems. The process was formalized in June 2016.

### ***Multi-factor Authentication***

PBGC is transitioning toward Personal Identification Verification (PIV) cards for the authentication of all users accessing PBGC systems and programs. Logging in with a PIV card is more secure because it provides multi-factor authentication.<sup>5</sup> This approach requires more than one factor to verify an employee's login, for instance, a PIV card and a PIN number. As of June 30, 2016, [REDACTED] PBGC employees and contractors were required to use a PIV card/PIN combination for logical access within the Corporation Intranet boundary. For remote access, PBGC employees and contractors use either a hardware token<sup>6</sup> or a PIV card.

---

<sup>5</sup> Based on the Cybersecurity Act of 2015, the term "multi-factor authentication" means the use of not fewer than two authentication factors, such as something that is known to the user as a password or personal identification number, an access device that is provided to the user such as a cryptographic identification device or token, or a unique biometric characteristic of the user.

<sup>6</sup> Hardware tokens are used for multi-factor authentication.

## **B. A description of privileged users<sup>7</sup> logical access controls and multi-factor authentication**

The PBGC Enterprise Systems and Services Access Control process describes the authorizations required in order to grant access to the system. This process assists in standardizing, granting, and documenting the system and application access permissions necessary for a user to be able to perform their specific job duties. This includes the granting of access to standard production, development and workspace access outlined in the Standard Account procedures, as well as the granting of access to non-standard production and administrative accounts as outlined in the Non-Standard Account procedures.

Identification and Authentication standard (IA-2) of NIST SP 800-53 requires use of multi-factor authentication for network and local access to privileged accounts, and use of replay-resistant authentication mechanisms, such as challenges, time synchronous authentication or challenge-response one-time authenticators for network access to privileged accounts. As of June 30, 2016, [REDACTED] privileged users are required to use their PIV card/PIN combination for network authentication from their primary workstations. *See Appendix 4.*

## **C . Logical access controls and multi-factor authentication**

The Corporation uses logical access controls of AC and IA families of NIST SP 800-53 and multi-factor authentication to access covered systems with some exceptions. PBGC utilizes Plan of Action & Milestones (POA&Ms) to identify, assess, prioritize and monitor the progress of corrective actions pertaining to information security weaknesses. As of June 20, 2016, 18 AC and IA control weaknesses identified in PBGC's POA&Ms remained open. The Corporation is at various stages of addressing these weaknesses. PBGC is also in the process of implementing PBGC OIG logical access recommendations from prior audits, reviews and evaluations. The Corporation recently submitted responses to close these recommendations. *See Appendices 5 and 6.*

## **D . A description of the security management practices**

We also reviewed PBGC's security management practices, including PBGC's capabilities, specifically, data loss prevention, forensic, visibility, and digital rights management capabilities, to detect and monitor threats such as exfiltration. The Cybersecurity Act of 2015 requires OIGs to describe their agencies capabilities in these areas. OIGs are also to describe their agencies

---

<sup>7</sup> Based on the Cybersecurity Act of 2015, the term "privileged user" means a user who has access to system control, monitoring, or administrative functions.

policies for performing inventories for software, software licenses and capabilities in detecting and monitoring threats such as exfiltration.

### ***Software Management***

PBGC's use of IT resources directive states the Corporation's objective to maintain licensing compliance for all software within the Corporation. Similar to the Corporation's logical access controls, PBGC's policies governing the inventorying of software are multi-tiered with directives and procedures. PBGC Property Management Directive, GA 10-3, requires the OIT to maintain an inventory of IT equipment and software and conduct an annual Corporation-wide inventory.

OIT supplements these directives with additional procedures and tools to perform and maintain the inventory of software and licenses. OIT's Information Technology Asset Life Cycle Functional Procedures Guidebook describes OIT's asset management procedures that are applicable to all PBGC information technology resources from acquisition through retirement, including software. The procedure calls for a software librarian to accept delivery, monitor, and track software by entering the information into the asset management software. The entry includes the name of the requestor for the software and license information.

Software maintenance contracts are also required to be tracked in the system. The guidebook includes instructions for the disposal of media and retiring software licenses when software is retired because it has reached the end of its useful life or based on management decision. However, PBGC officials indicated the guide's process to verify software license counts, utilization, and availability in conjunction with granting application access is no longer applicable due to the transition to enterprise licensing. Enterprise licenses are reviewed annually with vendors. Software that does not have enterprise licensing available is handled on an ad hoc basis. In the FY 2015 Vulnerability and Penetration Report, PBGC's OIG independent public accountant identified the need for better end-of-service-life transitions and multiple instances of unsupported software.

### ***Information Security Management Tools and Practices***

PBGC uses multiple tools to prevent data loss, to provide visibility to its security posture and to perform forensic analysis. However, PBGC does not have specific digital rights management capabilities implemented to prevent the unauthorized review, redistribution or modification of information outside the capabilities listed in Diagram 1. PBGC officials stated that the Corporation is licensed for Azure rights management service as part of Office 365 but does not have official plans to implement the service citing the need to consider the usability and security implications first. PBGC officials stated that the Corporation is improving its ability to



add data level protection, recognizing the importance of digital rights management, and plans to prioritize utilizing federal digital rights management share services when they are offered.

PBGC has implemented multiple tools in the other areas. Data loss prevention software and other tools prevent data from being exfiltrated and safeguard data in transit and at rest. PBGC also uses web proxies, vulnerability scanners, configuration management tools, intrusion detection systems and antivirus software to provide visibility of activities at the network, system, and workstation levels. Tools that are used on an as needed basis include software for memory capture, identification and removal of malicious software, security testing of web applications, and analysis of processes and connections. Diagram 1 lists the tools that provide data loss prevention and forensic and visibility functionality.

Diagram 1. PBGC Monitoring and Detection Capabilities

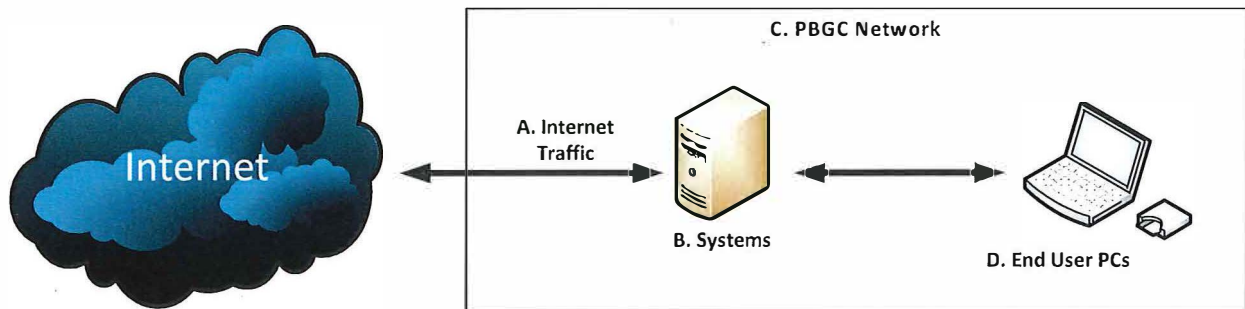


Diagram 1 Location	Purpose	Tool	Capability
■	Data Loss Prevention	■	■
		■	■
		■	■
■	Data Loss Prevention/ Monitoring and Visibility/ Forensic	■	■
		■	■
■	Monitoring and Visibility/ Forensic	■	■
		■	■
		■	■
		■	■
		■	■
		■	■

Diagram 1 Location	Purpose	Tool	Capability
	Monitoring and Visibility/ Forensic		

In addition to these tools, the Corporation contracted with a vendor to perform a compromise assessment of its environment. This assessment focused on workstations and servers and found no evidence of targeted attacker activity within the PBGC environment.

#### **E . A description of the policies and procedures for provided services**

PBGC does not have any policies or procedures that explicitly require entities providing services to PBGC to have policies and procedures to conduct inventories of software and associated licenses or to employ capabilities for data loss prevention, digital rights management, and forensic and visibility capabilities. However, these controls are indirectly required by the *Corporation's Security Requirements for All Contracts Involving PBGC Information and Information Systems* policy. It requires PBGC directives, NIST guidance, and appropriate clauses to be incorporated into procurement actions. These requirements ensure that the systems comply with the appropriate security controls found in NIST SP 800-53 or FedRAMP which cover these capabilities. Further, the PBGC Risk Management Framework Process defines responsibilities and accountability for security and privacy controls, and requires that vendor-hosted systems that process controlled unclassified information, such as PII, comply with NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*.

## **Appendix 1**

### **Objectives**

The objective of this evaluation is to report to the appropriate committees of jurisdiction in the Senate and the House of Representatives on PBGC's information system security policies and procedures governing systems and programs that provide access to PII and, specifically, to include the following:

- A. A description of the logical access policies and practices used by PBGC to access a covered system, including whether appropriate standards were followed.
- B. A description and list of the logical access controls and multi-factor authentication used by PBGC to govern access to covered systems by privileged users.
- C. A description of the reasons for not using such logical access controls or multi-factor authentication if applicable.
- D. A description of the information security management practices used by PBGC regarding covered systems, including the policies and procedures followed to conduct inventories of the software present on the covered systems and the licenses associated with such software, and the capabilities of PBGC to monitor and detect exfiltration and other threats.
- E. A description of PBGC policies and procedures with respect to ensuring that entities, including contractors, that provide services to PBGC are implementing the information security management practices described in part (D).

### **Scope and Methodology**

To accomplish our objectives, we:

- Reviewed the Federal Information Security Modernization Act of 2014 and applicable standards of NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* and NIST Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*;
- Obtained and reviewed PBGC's Information Security Policy, Information Security Standards, OIT Standard Operating Procedures, and other logical access processes and practices;

- Obtained and reviewed PBGC's *Security Requirements for All Contracts Involving PBGC Information and Information Systems, Property Management Directive, Use of Information Technology Resources Directive* and OIT's *Information Technology Asset Life Cycle Functional Procedures Guidebook*;
- Obtained a list of logical access controls used by privileged users and verified that these controls are documented in the appropriate policies and standards if applicable;
- Reviewed PBGC's Privacy Impact Assessments and System documentation;
- Interviewed PBGC and contractor personnel;
- Obtained and reviewed documentation of the application of PBGC's IT security management practices;
- Reviewed PBGC's OIG open recommendations related to information security;
- Reviewed and analyzed the Corporation's POA&Ms for open weaknesses in AC and IA control families.

Our work was performed at PBGC headquarters in Washington, D.C. from March through August 2016. The evaluation was conducted in accordance with the Quality Standards for Inspections and Evaluations established by the Council of the Inspectors General on Integrity and Efficiency, as well as applicable OIG policies and procedures. These standards require that we plan and perform the evaluation to obtain sufficient, competent and relevant evidence to provide a reasonable basis for our conclusions based on our evaluation objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our evaluation objectives.

We did not have any findings. We briefed responsible officials, but did not obtain the formal comments to this evaluation report. As requested by section 406 of the Cybersecurity Act of 2015, the scope of our work was limited to obtaining and analyzing PBGC's information security policies, practices and procedures governing computer systems that provide access to PII. We did not test the Corporation's internal controls or compliance with the policies and procedures provided in this report. Information on whether the Corporation followed the appropriate standards was based on OIG open recommendations and the Corporation's POA&Ms. We analyzed computer-processed data obtained from PBGC personnel. We reviewed related documentation, interviewed PBGC officials and performed comparisons of data. Based on the procedures performed we believe that the information used is valid and reliable for this evaluation.



## Appendix 2: PBGC Information Security Standards

PBGC directive, policy, or standard	Purpose	NIST Controls or Other Authority Addressed
PBGC External Information Systems and Services Standard (SE-STD-01-02)	The standard defines the requirement to establish terms and conditions with other organizations that own, operate, or maintain external information systems and the requirement that providers of external information system services comply with PBGC information security requirements, employing appropriate security controls in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance.	<ul style="list-style-type: none"> <li>• Use of External Information System (AC-20)</li> </ul>
PBGC Public Information Security Standard (SE-STD-01-03)	The standard defines the requirement to identify, document, and control actions permitted without identification or authentication; securely manage publicly accessible content; and protect the integrity and availability of publicly available information systems.	<ul style="list-style-type: none"> <li>• Actions Permitted Without Identification or Authentication (AC-14)</li> <li>• Publicly Accessible Content (AC-2)</li> </ul>
PBGC System Privilege Standard (SE-STD-01-04)	The standard defines the requirements for separation of duties and least privileges.	<ul style="list-style-type: none"> <li>• Separation of Duties (AC-5)</li> <li>• Least Privilege (AC-6)</li> </ul>
PBGC Identification and Authentication Standard (SE-STD-01-27)	The standard defines the requirement to uniquely identify and authenticate PBGC users; uniquely identify and authenticate specific types of devices before establishing a connection; manage information system identifiers for users and devices by receiving authorization from a designated PBGC official; manage information system authenticators for users and devices by verifying their identity; and uniquely identify.	<ul style="list-style-type: none"> <li>• Identification and Authentication (Organizational Users) (IA-2)</li> <li>• Device Identification and Authentication (IA-3)</li> <li>• Identifier Management (IA-4)</li> <li>• Authenticator Management (IA-5)</li> <li>• Authenticator Feedback (IA-6)</li> <li>• Cryptographic Module Authentication (IA-7)</li> <li>• Identification and Authentication (Non-Organizational Users) (IA-8)</li> </ul>
PBGC Access Control Standard (SE-STD-01-32)	The standard defines the requirements related to identifying authorized users of the information system and specifying access privileges. It defines the requirement for information systems to enforce approved authorizations for logical access to the system; the requirement for information systems to enforce authorizations for controlling the flow of information within the system and between interconnected systems; the requirement for PBGC information systems to display an approved system use notification message or banner before granting access to nonpublic systems and when appropriate for public systems; and the requirement to define usage restrictions and implementation guidance for wireless access. In addition, it defines requirements related to access control for mobile devices and the requirement to prohibit remote activation of collaborative computing mechanisms and explicit indication to the local users that devices are in use.	<ul style="list-style-type: none"> <li>• Account Management (AC-2)</li> <li>• Access Enforcement (AC-3)</li> <li>• Information Flow Enforcement (AC-4)</li> <li>• Unsuccessful Login Attempts (AC-7)</li> <li>• System Use Notification (AC-8)</li> <li>• Session Lock (AC-11)</li> <li>• Remote Access (AC-17)</li> <li>• AC-18 Wireless Access (AC-18)</li> <li>• Access Control for Mobile Devices (AC-19)</li> </ul>
PBGC OIT Identity, Credential, and Access Management (ICAM) Interim Standard (SE-STD-01-34)	<p>The purpose of this Interim Standard is to outline a common framework for ICAM within the PBGC and to identify policies and guidance for PBGC and its information systems for term implementation. In support of the overall purpose, the interim standard was written to accomplish the following objectives:</p> <ul style="list-style-type: none"> <li>• Present an overview of identity, credential, and access management to ensure consistent understanding across PBGC stakeholders;</li> <li>• Illustrate the key players and compliance initiatives involved in program;</li> <li>• Give guidance on how to incorporate a segment architecture for program;</li> <li>• Provide a high-level vision for the target state of PBGC's use and management of services; and</li> <li>• Provide design standards that are applicable to ICAM Services in the interim.</li> </ul>	<ul style="list-style-type: none"> <li>• Homeland Security Presidential Directive 12 (HSPD-12)</li> <li>• Federal Information Security Management Act of 2002</li> <li>• Federal ICAM Roadmap</li> </ul>

### Appendix 3: Standard Operation Procedures

SOP	Purpose	Scope and Applicability	Partially or fully Addressed NIST controls
+			
+			
+			
+			

#### Appendix 4: Privileged Users Controls

NIST Control	Privileged Users Control Description
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



## Appendix 5: Plan of Action and Milestones

System Name	System Type	POA&M Title	Detailed Weakness Description
ITISGSS	GSS	AC-2: Account Management and Standardization	ITISGSS user accounts are not managed effectively and consistently. Temporary accounts are prohibited in practice, but not in procedure or policy.
ITISGSS	GSS	AC-2, AC-2(4), AC-7: Automated Response to Dormancy and Separation	Automation does not effectively support account management. Emergency accounts are not always automatically terminated, and inactive accounts are not always automatically disabled when discovered via dormancy reports or separation processing notifications.
ITISGSS	GSS	AC-6, DM-3: Data Masking	PII is currently being used in the development and test environment. SOURCE: FISMA-11-02 (NFR 38)
ITISGSS	GSS	AC-5, AC-6: Separation of Duties and Least Privilege	The user role structure does not adequately implement separation of duties and does not associate required functions with adequate authorized access.
ITISGSS	GSS	AC-19, AC-20(2), MP-5, MP-6, MP-7: Removable Media and Mobile Device Control	PBGC's removable media and mobile device control procedures are not in alignment with best practices and security control guidance. Tracking, sanitizing, encrypting in transit, and restricting use are not adequately addressed.
ITISGSS	GSS	AC-2, PS-6: Access Agreements	User accounts and associated user access agreements are not reviewed and updated periodically.
ITISGSS	GSS	AC-3, CM-6, CM-7: Least functionality, security hardening, and network access control	Components' intended roles/functions are not associated with their default capabilities, and configuration settings do not implement least functionality, security hardening and industry best practices, and do not control access to the network.
ITISGSS	GSS	AC-3: SharePoint Usage Policy and Restrictions	Usage policy and guidelines for the use of PBGC Connect (SharePoint) sites have not been established, distributed, trained and enforced, and do not adequately address protection requirements for sensitive data.
ADM	System	AC-5: Separation of Duties	The main system administrator is responsible for adding accounts to the ADM system and creating initial passwords to the system as well as reviewing system logs. The same system administrator should not be responsible for administering access control functions and audit functions, this could create a scenario where access changes could be made and either inadvertently or advertently hidden from detection by other system personnel.
ITISGSS	GSS	AC-1, AC-2: Account Recertification Enforcement	The procedure for performing account recertification does not require and/or enforce removal of accounts or privileges that are no longer required.
MyPAA	System	AC-2(3): Account Management   Disable Inactive Accounts - My PAA - Customer	The FOD plans to improve the automated process to deactivate Customer Module user accounts. The automated process to deactivate accounts should be based on an individual users last login date; specifically, the My PAA Customer Module does not currently deactivate inactive accounts associated with a delayed filing when there is the potential that individual user accounts should be deactivated.
RMEW	System	AC-1: Access Control Policy and Procedures	RMEW states it utilizes the "Enterprise Process" for access control procedures. RMEW has no access control procedures for AC-1, and therefore has not distributed access control procedures to RMEW personnel, and does not review and update those procedures annually. The Common Control Provider outlined the "IT Process, IO-PRO-03-02" as procedures to facilitate the implementation of the access control policy and associated access control controls. Reviewed PBGC PPL, IO-PRO-03-02 no longer exists in the PPL. Determine from ECD if procedures are needed for AC-1 or to document steps that use Enterprise process for applicable AC family controls (AC-6(5) and AC-12). Distribute to personnel, review and update annually.
LTP	Program	AC-12 (1,2) Automatically terminates a user session after organization-defined conditions	Provide proof that LTP is complying with this control.



## Appendix 6: PBGC's OIG Open Audit and Evaluation Recommendations for Logical Access Controls

Rec Number	Issued	Report Title	Corporation Expected Completion	Response Received	Recommendation
FISMA-11-02	5/30/2012	Fiscal Year 2011 Federal Information Security Management Independent Evaluation Report	6/30/2016	6/29/2016	Remove PII from the development environment.
FISMA-14-15	5/6/2015	Fiscal Year 2014 Federal Information Security Management Act Independent Evaluation Report	6/30/2016		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.
FS-07-08	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit	6/30/2016	6/30/2016	Remove unnecessary user and/or generic accounts.
FS-07-10	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit	6/30/2016	6/30/2016	Appropriately restrict developers' access to production environment to only temporary emergency access.
FS-07-12	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit	6/30/2016	6/30/2016	For the remaining systems, apply controls to remove/disable inactive and dormant accounts after a specified period in accordance with the PBGC Information Security Policy (formerly Information Assurance Handbook-IAH).
FS-07-14	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit	6/30/2018		Implement controls to remedy vulnerabilities noted in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating systems access.
FS-09-12	11/12/2009	Report on Internal Controls Related to PBGC's Fiscal Year 2009 and 2008 Financial Statements Audit	6/30/2016	6/30/2016	Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems.
OIT-149	8/6/2015	PBGC Began Developing Methods for Oversight and Administration of Cloud Computing Service Providers – Work is Needed for the Expected Increase in Externally Hosted Systems	6/30/2016	6/21/2016	Establish, implement and monitor controls which provide reasonable assurance that foreign personnel with access to PBGC data and information systems receive background checks in accordance with PBGC policy and procedures.
FS-15-04	11/13/2015	Report on <u>Internal Controls Related</u> to PBGC's Fiscal Year 2015 and 2014 Financial Statement Audit	12/31/2016		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.
OIT-153R	12/11/2015	Fiscal Year 2015 Vulnerability Assessment and Penetration Testing Report	6/30/2017		Develop plans to identify, protect weak authentication protocols, and change default passwords.
FISMA-15-06	2/19/2016	Fiscal Year 2015 Federal Information Security Modernization Act Final Report	6/30/2017	6/30/2016	Ensure that password and account lockout settings for databases are updated to be consistent with PBGC requirements identified in the PBGC Identification and Authentication Standard (SE-STD-01-27) and PBGC Access Control Standard (SE-STD-01-32).