Pension Benefit Guaranty Corporation

Directive

Subject: PBGC Information Security Policy

Directive Number: IM 05-02

Originator: OIT

JANET DHILLON

Digitally signed by JANET DHILLON
Date: 2026.10.13 09:56:06 -04'00'

Janet Dhillon
PBGC Director

1. **PURPOSE**: This Directive authorizes the Pension Benefit Guaranty Corporation (PBGC) to establish and maintain an enterprise cybersecurity program, including the information security policy, in accordance with the federal laws and guidelines in order to protect PBGC information systems, assets, and data.

2. **EFFECTIVE DATE**: This Directive replaces PBGC Directive IM 05-02, dated 05/08/2023. This Directive is effective on the date shown above.

3. **SCOPE**: This Directive applies to all PBGC employees and contractors and to all PBGC information systems that store, process, or transmit PBGC information.

4. **AUTHORITIES**:
   a. Executive Order No. 14434, 91 FR 63129, Inaugurating the Era of Super Intelligence (September 29, 2026)
   b. Off. of Mgmt. & Budget, (OMB) Memo M-26-15, Execution of the Migration to Post-Quantum Cryptography (June 24, 2026)
   c. Executive Order No. 14412, 91 FR 38483, Securing the Nation Against Advanced Cryptographic Attacks (June 22, 2026)
   d. Executive Order No. 14409, 91 FR 34565, Promoting Advanced [Super] Intelligence Innovation and Security (June 2, 2026)
   e. Off. of Mgmt. & Budget, (OMB) Memo M-26-14, Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats (May 22, 2026)
   f. Off. of Mgmt. & Budget, (OMB) Memo M-26-05, Adopting a Risk-based Approach to Software and Hardware Security (January 23, 2026)
   g. Executive Order No. 14306, 90 FR 24723, Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144 (June 6, 2025)
   h. Executive Order No. 14144, 90 FR 6755, Strengthening and Promoting Innovation in the Nations Cybersecurity (January 16, 2025)
   i. Off. of Mgmt. & Budget, (OMB) Memo M-24-15, Modernizing the Federal Risk and Authorization Management Program (FedRAMP) (July 25, 2024)

j. Off. of Mgmt. & Budget, OMB M-25-21, Accelerating Federal Use of [SI] through Innovation, Governance, and Public Trust (2025)
k. Executive Order No. 14117, 89 FR 15421, Preventing Access to Americans' Bulk Sensitive Personal Data (February 2024)
l. Executive Order No. 14028, 86 FR 26633, Improving the Nation's Cybersecurity (May 12, 2021)
m. Off. of Mgmt. & Budget, (OMB) Memo 22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022)
n. Off. of Mgmt. & Budget, OMB Circular A-130, Management of Federal Information Resources (1996)
o. Off. of Mgmt. & Budget, (OMB) Revision Circular A-130, Managing Information as a Strategic Resource (2016)
p. Off. of Mgmt. & Budget, (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget, §25.5; 51.19 (revised 2025)
q. Clinger-Cohen Act, Pub. L. No. 104-106, 110 Stat 186 (1996)
r. Federal Information Security Modernization Act (FISMA), 44 U.S.C. §3551, et seq., Pub. L. 113-283) (2014)
s. The Privacy Act, 5 U.S.C. § 552a (1974)
t. Executive Order No. 13556, 75 FR 68675, Controlled Unclassified Information (CUI) (2010)
u. Controlled Unclassified Information, 32 C.F.R. §2002 (2016)
v. Federal Records Act of 1950 as amended 44 U.S.C. Chapter 31
w. Foundations for Evidence-Based Policymaking Act, Pub. L. No. 115-435(2019)
x. Nat'l Inst. of Standards & Tech., Federal Information Processing Standard Publ'n199, Standards for Security Categorization of Federal Information and Information Systems (2004)
y. Nat'l Inst. of Standards & Tech., Federal Information Processing Standard Publ'n 200, Minimum Security Requirements for Federal Information and Information Systems (2006)
z. Nat'l Inst. of Standards & Tech., Federal Information Processing Standard Publ'n 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors (2022)
aa. Nat'l Inst. of Standards & Tech. Special Publications (NIST SP):
    (1) NIST SP 800-30, Guide for Conducting Risk Assessments
    (2) NIST SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
    (3) NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
    (4) NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations
    (5) NIST SP 800-53B, Control Baselines for Information Systems and Organizations
    (6) NIST SP 800-53A, Assessing Security and Privacy Controls in Information Systems and Organizations
    (7) NIST SP 800-60, Vols. I and II, Guide for Mapping Types of Information and Information Systems to Security Categories

bb. PBGC Directive FM 15-03, Suspension and Debarment Program
cc. PBGC Directive IM 05-04, Use of Information Technology Resources
dd. PBGC Directive IM 05-07, Information Technology Management
ee. PBGC Directive IM 05-09, PBGC Privacy Program
ff. PBGC Directive IM 05-12, Recording Policy
gg. PBGC Directive IM 10-03, Protecting Personally Identifiable Information
hh. PBGC Directive IM 10-05, Media Relations
ii. PBGC Directive IM 10-07, Controlled Unclassified Information
jj. PBGC Directive IM 15-03, PBGC Records Management Program
kk. PBGC Directive PM 30-01, Disciplinary and Adverse Procedures
ll. PBGC Office of Information Technology Glossary of Terms

5. **BACKGROUND**: PBGC requires that all information systems (regardless of location or delivery mechanism) abide by the information security policies set forth in this Directive to ensure the confidentiality, integrity, and availability of data in PBGC information systems. The Federal Government has instituted several laws, regulations, and directives that govern the establishment and implementation of Federal information security practices. These laws, regulations, and directives establish Federal and agency-level responsibilities for information security, define key information security roles and responsibilities, identify minimum information security controls, specify compliance with reporting rules and procedures, and provide other essential requirements and guidance. These laws and regulations place responsibility and accountability for information security at all levels within Federal agencies, from agency heads to the information technology users.

Additionally, the policies defined within are designed to facilitate commonality in the planning, implementing, monitoring, and reporting of information security requirements and to be used as a reference by information system owners, project managers, and other responsible Federal and contractor staff. These policies are organized in accordance with NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations.

The PBGC Information Security Policy Directive (hereinafter Directive) sets the policy direction for safeguarding electronic information and information systems from various threats while demonstrating successful program stewardship to the Federal Government. It also enables PBGC information assets to be protected in a manner commensurate with mission importance, threat environments, known vulnerabilities, and consequences of loss for the information it processes. This Directive also puts in place the guidelines that:

a. Establishes the Risk Management Framework (RMF) is aligned with the most recent versions of:
   (1) NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View.
   (2) NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.

b. Protects PBGC information and information assets in a cost-effective manner by managing information security, records management, CUI, and privacy risks, considering mission priorities, and allocating resources to the most efficient solutions necessary to reduce risk to acceptable levels.
c. Considers the need to synchronize mission execution and performance with business, information technology (IT) infrastructure, and information security, privacy, records management and CUI requirements.
d. Provides flexibility to tailor and implement risk mitigation controls considering threats, acceptable risks, mission needs, and environmental and operational factors.
e. Integrates Enterprise Architecture (EA) processes and procedures with information security, records management, CUI, and privacy.

6. **POLICY**: It is PBGC policy to protect its information and information systems in a manner commensurate with the level of risk, sensitivity, value, and criticality of the information. PBGC shall:

a. Implement a multi-level cybersecurity risk management process to protect pensioner information, PBGC operational capabilities, and PBGC individuals, organizations, and assets at the PBGC Enterprise level, through the PBGC Business Units, down to the information systems level as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39.

b. Categorize all PBGC information systems that process, store, or transmit PBGC data and information, including externally owned and hosted systems in accordance with Federal Information Processing Standard (FIPS) 199, implement a corresponding set of information security and privacy controls from the current version of NIST SP 800-53, NIST 800-53B, and use assessment procedures from NIST SP 800-53A and PBGC organization-defined control parameters, implementation guidance, and processes and procedures found on the Office of Information Technology (OIT) Process and Procedures Library (PPL).

c. Address risk management by incorporating information security requirements as early as possible in the acquisition or development of IT and in an integrated manner across the IT life cycle.

d. Leverage the Joint Cybersecurity Authorization Management (JCAM) tool as the authoritative source for PBGC information system authorizations and common control programs. All system assessment and authorization artifacts, risk remediation plans and related information shall be stored within JCAM. PBGC's enterprise common controls and organization-defined control parameters shall also be stored within JCAM, and inheritance of common controls shall be documented within the tool.

e. Utilize JCAM for Plans of Actions and Milestones (POA&M) management for remediations of audit findings and recommendations.

f. Establish a process to deploy privacy, records management, CUI, and information security controls throughout PBGC consistent with the provisions of NIST SP 800 Series, FIPS, other applicable federal mandates, and the PBGC RMF. These processes will facilitate implementation of Directive IM 05-02 and associated NIST 800-53 controls.

g. Comply with standards, organizationally defined parameters, procedures, processes, and guidance developed and disseminated by the Enterprise Cybersecurity Department (ECD), the Privacy Office, the Controlled Unclassified Information (CUI) Senior Agency Official (CUI SAO), the Senior Agency Official for Records Management (SAORM) and the Cybersecurity and Privacy Council to address privacy, records management, CUI, and information security compliance, responsibilities, management commitment, and coordination among organizational entities. Standards, processes, procedures, and guidance derived from this Directive are an extension of this policy.

h. Disseminate procedures to facilitate implementation of this Directive and associated controls.

7. **POLICY DEVIATIONS**:

a. The Chief Information Security Officer (CISO), Senior Agency Official for Privacy (SAOP) will collectively approve IT information security policy deviations and will include the CUI Senior Agency Official (CUI SAO) and Senior Agency Official for Records Management (SAORM) if CUI or records management is involved. IT security policy deviation requests will be submitted by an Information System Security Manager (ISSM), Information System Owner (ISO), or Authorizing Official (AO) and adhere to this Policy Deviation Process.

b. Deviation request memorandum will include:
   (1) Program, IT Project, or System requesting exemption;
   (2) Identification of the issue or vulnerability;
   (3) Requirements needing waiver;
   (4) Steps taken to reduce, mitigate, or compensate for the risk;
   (5) Risk acceptance for residual risks if exemption is granted;
   (6) Benefits to the organization by providing the exemption;
   (7) Identification of other pertinent data for obtaining an exemption.

c. Approved deviations will be stored and reviewed in PBGC's security documentation system of record on an annual basis through the Annual Security and Privacy Assessment and Authorization Process.

d. Approved deviation requests will be uploaded as an artifact within the JCAM Status and Archive Page.

e. Any change in the underlying risks that led to the approved policy deviation

should be reported to the CISO, SAOP, CUI SAO, and SAORM as soon as practicable for a determination on whether the approved deviation is still valid and necessary.

f. Policy deviations involving privacy issues must comply with the requirements set forth in Directive IM 05-09. Policy deviations impacting CUI must comply with requirements set forth in Directive IM 10-07 and PBGC's CUI Program Intranet Page. Policy deviations impacting records and information management must comply with requirements set forth in Directive IM 15-03 and PBGC's Records and Information Management Intranet Page.

8. **NON-COMPLIANCE**:

a. Individuals found to be non-compliant with this policy may be subject to a review in accordance with the following:
   (1) Employee discipline under Directive PM 30-01.
   (2) Contractor suspension or debarment under Directive FM 15-03.
   (3) Removal of an individual's authority to access PBGC information systems.

b. PBGC information systems are required to have a current Information Security/Cybersecurity Authorization designated by an Authorizing Official. A system that is found to be non-compliant with this policy will be subject to Chief Information Officer (CIO), Senior Agency Official for Privacy (SAOP), Senior Agency Official for Records Management (SAORM), and CUI Senior Agency Official (CUI SAO) for review and action.

9. **DEFINITIONS**:

a. **Assessment and Authorization (A&A)**. The process of conducting a security assessment on a system and determining, based on the results of that assessment, whether the system should be given a security authorization.
b. **Common Control.** A control that is inheritable (usable) by one or more organizational information systems.
c. **Control**. A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined information security requirements. The controls establish a linkage and relationship between privacy, records management, CUI, and information security controls for purposes of enforcing respective privacy, records management, CUI and information security requirements which may overlap in concept and in implementation within PBGC information systems.
d. **Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
e. **Organizational-Defined Control Parameter (ODP).** The variable part of a control or control enhancement that is instantiated by an organization during the tailoring process by either assigning an organization-defined value or selecting a value from a predefined list provided as part of the control or

control enhancement.

f. **Plan of Action and Milestones (POA&M).** A process that identifies tasks that need to be accomplished. It details tasks required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist PBGC in identifying, prioritizing, and monitoring the progress of corrective actions for weaknesses found in programs and systems.

g. **Risk.** The probability and impact of damage, injury, liability, loss, or any other negative effect that is caused by a threat agent exploiting a technical, procedural, or organizational (i.e., lack of resources or management oversight) weakness or vulnerability.

h. **Risk Management.** The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system. This includes assessing information system risks, implementing risk mitigation strategy, and employing continuous monitoring to consistently assess the information security state of the information system.

i. **Rules of Behavior.** Establishes the rules that describe the responsibilities and expected behaviors about information and information system usage.

j. **Security Authorization.** The notice to proceed with the "live" system. It is the official management decision given by a system's Authorizing Official (AO) who authorizes operation of an information system and explicitly accepts the risk to PBGC operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of information security controls. Security Authorizations are referred to as an "Authority to Operate (ATO)" or "Authority to Use (ATU)."

k. **Vulnerability.** Weakness in an information system, information system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

10. **PROCESSES**: Cybersecurity documents utilized for implementing privacy, records management, CUI, and information security controls will be described in the PBGC Information Security Risk Management Framework (RMF) Process. The vetting and publication of cybersecurity documents will be governed by the Office of Information Technology's Governance Coordination Board (GCB). Cybersecurity documents are published on PBGC's intranet and on the OIT PPL**.** Published documents, including the PBGC RMF Process document, will be reviewed on an annual basis. Unless otherwise noted, stakeholders noted in the Responsibilities section of this Directive shall receive notice after cybersecurity documents are published. Cybersecurity documents shall be implemented 180 days after publication.

11. **RESPONSIBILITIES**:
This Directive lays out the responsibilities of selected roles. A complete list of roles and most recent responsibilities are listed in the Information Security RMF Process.

a. **PBGC Director.**

(1) Retains overall responsibility and accountability for information security protections commensurate with the risk and impact of harm to the PBGC's operations, assets, and individuals within the organization.

(2) Ensures development and implementation of policies to establish PBGC's commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions performed by PBGC.

(3) Appoints the chair of the Risk Management Council (RMC).

b. **Chief Information Officer (CIO).**

(1) Provides advice and other assistance to the PBGC Director and other senior officials to ensure that information technology (IT) is acquired, and information resources are managed for the agency in a manner that is consistent with the Clinger-Cohen Act and FISMA.

(2) Designates a Chief Information Security Officer (CISO) to execute the Cybersecurity Program.

(3) Designates the Authorizing Official for the management and oversight of PBGC information systems.

(4) Ensures development and implementation of policies for information security and the effective management of risk to protect the core missions and business functions performed by PBGC.

c. **Chief Information Security Officer (CISO).**

(1) Develops, documents, and implements an agency-wide cybersecurity program to provide information security for the information and information systems that support the operations and assets of the agency in the most cost-effective manner and in compliance with Federal mandates.

(2) Ensures departments are informed of the total cost of ownership requirements required to support this Directive in a timely manner to support resource justifications.

(3) Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements for protecting PBGC information and information systems.

(4) Assists senior PBGC officials in performing their information security responsibilities.

(5) Develops, maintains, authorizes, and manages a PBGC enterprise RMF.

(6) Designates the Common Control Provider for the management and oversight of common controls (i.e., security controls inherited by information systems).

(7) Oversees the Enterprise Common Controls and associated organizational-defined control parameters on behalf of the agency.

(8) Reviews and approves IT security policy deviations where appropriate.

(9) Provides mandatory cybersecurity training for PBGC employees and contractors, at the time of hiring/onboarding and on an annual basis, to make them aware of the policies and procedures for protecting sensitive information.

(10) Designates the Information System Security and Privacy Officer (ISSPO) and Information System Security Manager (ISSM) for management of PBGC systems.
(11) Oversees an agency-wide Cybersecurity Supply Chain Risk Management (C-SCRM) Program.
(12) Serves as Co-Chair of the Cybersecurity and Privacy Council.

d. **Senior Agency Official for Privacy (SAOP).**
(1) Ensures implementation of information privacy protections, including full compliance with Public Laws, regulations, and policies relating to information privacy, such as the Privacy Act.
(2) Ensures privacy control requirements are met through the RMF lifecycle, including categorization of systems pursuant to the FIPS 199, so that FISMA reportable systems maintain their Security Authorization.
(3) Participates in agency information privacy compliance activities (i.e., privacy policy as well as information policy).
(4) Participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals.
(5) Participates in assessing the impact of technology on the privacy of personal information.
(6) Reviews privacy procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and federal guidance.
(7) Consults and collaborates with the appropriate PBGC departments in identifying, developing, adopting, and implementing, as needed, additional or revised privacy procedures.
(8) Ensures that employees and contractors receive appropriate training and education regarding their privacy protection responsibilities.
(9) Prepares and submits various privacy related reports, such as the annual Senior Agency Official Privacy Report to OMB required by FISMA.
(10) Reviews and approves cybersecurity policy waiver deviations where appropriate.
(11) Works closely with the CIO and CISO to reduce the exposure of Personally Identifiable Information (PII) in PBGC information systems and in the conduct of PBGC business, and to reduce the holdings of PII, including the use of Social Security Numbers, whenever possible.
(12) Designates the ISSPO for management of PBGC information systems.

e. **Chief Privacy Officer (CPO).**
(1) Initiates, facilitates, and promotes activities to foster information privacy awareness within PBGC, especially regarding sensitive information.
(2) Develops and supports privacy protection policies and procedures.
(3) Assists PBGC departments in achieving and maintaining compliance with the Privacy Act, the Freedom of Information Act (FOIA), and other relevant legal authorities.
(4) Provides guidance to PBGC departments and employees regarding privacy matters.

(5) Develops and presents training on protecting PII to new hires, employees, and contractors.
(6) Provides guidance to information system owners on conducting Privacy Impact Analyses (PIAs) and Privacy Threshold Assessments (PTAs).
(7) Develops and provides guidance on drafting and maintaining accurate System of Records Notices (SORNs).
(8) Receives and responds to questions and concerns regarding PBGC's privacy policies and procedures.
(9) Receives, documents, tracks, and addresses all suspected and confirmed privacy breaches, including reporting to the Cybersecurity and Infrastructure Security Agency (CISA) when required, and notifying impacted individuals when appropriate.
(10) Serves as Co-Chair of the PBGC Cybersecurity and Privacy Council.

f. **CUI Senior Agency Official (CUI SAO).**
(1) Primarily responsible for the PBGC CUI policy and exercises a significant role in overseeing, coordinating, resourcing, and facilitating the organization's compliance efforts with the CUI Program.
(2) Provides guidance to the PBGC Director and senior leadership to ensure that CUI is handled and protected in a manner which complies with applicable laws, regulations, government-wide policy, and EA guidance.
(3) Designates a CUI Program Manager (PM) in writing.
(4) Ensures the organization's CUI procedures are comprehensive, current, and compliant with applicable laws and Federal guidance.
(5) Consults and collaborates with the appropriate PBGC offices in developing, adopting, and implementing newly identified and revised CUI procedures.
(6) Ensures PBGC federal employees and contractors receive appropriate training and education regarding their CUI handling and protection responsibilities.
(7) Coordinates with the CISO, CIO, SAOP, and other relevant stakeholders as needed to respond to CUI incidents involving federal information systems which are non-compliant with this Directive.
(8) Reviews and settles deviations from PBGC's CUI policy.
(9) Works closely with the CISO and CIO who have Information System security responsibilities.
(10) Serves as the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI Executive Agent (EA).
(11) Notifies authorized recipients, the CUI EA, and the public of any waivers granted by PBGC, including a description of all waivers in the annual report to the CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps PBGC is taking to ensure sufficient protection of CUI within the agency.
(12) Develops and implements PBGC's Self-Inspection program.

g. **Senior Agency Official for Records Management (SAORM).**

(1) Sets the vision and strategic direction for PBGC's records management program.

(2) Advocates for PBGC's records management program ensuring adequate resources are embedded into the agency's Strategic Information Resources Management (IRM) Plan.

(3) Ensures that the records management program documents the organization's activities and decisions.

(4) Ensures PBGC protects records against unauthorized removal or loss and ensures all agency staff are informed of their records management responsibilities.

(5) Submits reports to NARA, supporting records management inspections, and other oversight activities.

(6) Ensures agency staff are informed of and receive training on their records management responsibilities as defined in NARA regulations and guidance.

(7) Formally designates the Agency Records Officer (ARO) and informs NARA in writing of this decision.

(8) Ensures compliance with NARA requirements for electronic records.

(9) Ensures the agency efficiently and appropriately complies with all applicable records management statutes, regulations, NARA policy, and OMB policy.

(10) Promotes effective records management at a senior level by seeing across program offices in the deployment of individual IT systems.

(11) Coordinate PBGC's records management program with other related disciplines such as information security, risk management, data management, and knowledge management. This may also include programs related to discovery, privacy, and the Freedom of Information Act (FOIA).

(12) Integrates the records management program within PBGC's information framework as it develops and matures.

h. **CUI Program Manager (PM).**

(1) Primarily responsible for daily operations of the CUI Program and implementing PBGC's CUI policy, procedures, and compliance efforts.

(2) Develops and maintains the CUI Program's policies, procedures, processes, training, and controls to address all requirements set forth in federal law, regulations, and guidance.

(3) Implements CUI guidance and training in coordination with Contracting Officers, and technology requirements.

(4) Oversees and manages the program, waiver process, and reporting of activities related to CUI.

(5) Performs PBGC's agency-wide self-inspection to ensure ongoing compliance with National Archives and Records Administration (NARA) requirements.

(6) Identifies and designates the appropriate markings for protecting CUI in accordance with the CUI EA's guidance.

(7) Notifies the Contracting Officer Representative (COR) when a contractor fails to follow PBGC's policies and procedures for protecting and handling CUI.
(8) Notifies the federal manager or supervisor when a federal employee fails to follow PBGC's policies and procedures for handling CUI.
(9) Implements a mandatory CUI training program.
(10) Receives, documents, tracks, and addresses all suspected and confirmed incidents involving CUI, except for the reporting of cybersecurity and insider threat incidents and PII breaches.
(11) Keeps CUI SAO, SAOP, and CISO advised of CUI activities, as necessary.
(12) Assists PBGC departments in achieving and maintaining compliance with the CUI Program and other relevant legal authorities.
(13) Partners with the CPO to protect sensitive information in all formats.
(14) Receives and responds to questions and concerns regarding PBGC's CUI policies and procedures.

i. **Agency Records Officer (ARO).**
(1) Acts as the official liaison with NARA and responds to data calls and mandatory reports.
(2) Promotes, executes, implements, and maintains the PBGC records management program in accordance with records management statutes, regulations, NARA policy, and Presidential Directives.
(3) Develops standards, procedures, and guidance for improving PBGC's Records Management program.
(4) Communicates records management policies and procedures across the PBGC.
(5) Keeps senior management officials advised of records management activities.
(6) Ensures PBGC Records Schedule and NARA's various General Records Schedule (GRS) are current and accurate.
(7) Conducts periodic evaluations of PBGC's records management activities and records to ensure compliance and assess its operational, efficiency, and effectiveness of PBGC's records management program.
(8) Provides input and guidance regarding information technology requirements relating to records management:
(a) Records management requirements for all new or updated systems deployed.
(b) Proper retention and disposition of system records in all information systems, including scheduling of systems, as necessary.
(c) Ensure compliance with records management principles and policies in all phases of the Enterprise Performance Life Cycle (EPLC) process.
(9) Reviews language in cooperation with the Procurement Department and the Office of General Counsel for the off-site storage of federal records.

(10) Ensures mandatory records management training is conducted and completed annually (initially during the formal on-boarding process and annually thereafter) and refreshes training materials as needed.
(11) Facilitates records management Records Coordinator training.
(12) Notifies the Archivist of the United States of any actual, impending, or threatened unlawful destruction of records.
(13) Assists PBGC Departments with Records Management activities.

j. **Chief Data Officer.**
(1) Coordinates with the CISO and the CPO to ensure to the extent practicable, PBGC maximizes its use of data in areas including production of evidence, regulatory analyses, cybersecurity, and the improvement of agency operations.

k. **Enterprise Risk Management Team.**
(1) Leads the task of creating an Enterprise Risk Management (ERM) framework to ensure the agency has a consistent risk assessment approach.
(2) Encourages PBGC employees to communicate openly and freely about current and potential risks to the agency.
(3) Facilitates timely identification of PBGC's risks to help implement mitigation strategies before reaching full impact.

l. **Risk Management Council.**
(1) Coordinates a PBGC-wide Enterprise Risk Management (ERM) program.
(2) Acts as an advisory council to the Director and the Executive Management Committee (EMC) on strategic, operational, compliance, and reporting risks.

m. **Risk Executive (Function).**
(1) PBGC leverages the Risk Management Council along with input from the PBGC CIO, CISO, and SAOP to function as the Risk Executive function for the organization.
(2) Through the Risk Management Council, the Risk Executive function serves to:
(a) Establish risk management roles and responsibilities.
(b) Develop and implement an organization-wide risk management strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time).
(c) Manage threat and vulnerability information regarding organizational information systems and the environments in which the systems operate.
(d) Establish organization-wide forums to consider all types and sources of risk (including aggregated risk).
(e) Determine organizational risk based on the aggregated risk from the operation and use of information systems and the respective

environments of operation.

(f) Provide oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions.

(g) Develop a greater understanding of risk with regard to the strategic view of organizations and their integrated operations.

(h) Establish effective vehicles and serve as a focal point for communicating and sharing risk related information among key stakeholders internally and externally to organizations.

(i) Specify the degree of autonomy for subordinate organizations permitted by parent organizations with regard to framing, assessing, responding to, and monitoring risk.

(j) Promote cooperation and collaboration among authorizing officials to include information security authorization actions requiring shared responsibility (e.g., joint/leveraged authorizations).

(k) Ensure that information security authorization decisions consider all factors necessary for mission and business success.

(l) Ensure shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision making authorities.

n. **Chief Super Intelligence (SI) Officer.**

(1) Coordinates agency's use of SI.

(2) Promotes SI innovation within the agency.

(3) Manages risks from agency's use of SI.

(4) Serves as a senior advisor on SI to the head of the agency and within PBGC's executive decision-making forums.

(5) Represents the agency in and collaborates with coordination bodies related to agency SI activities.

(6) Maintains the agency's SI Use Case Inventory.

(7) Advises on the agency's workforce for SI.

(8) Ensures SI code and the data used to develop and test SI are appropriately inventoried, shared, and released in agency code and data repositories, in coordination with relevant agency officials.

(9) Supports efforts to track SI spending and resourcing.

o. **Cybersecurity and Privacy Council.**

(1) Provides a forum to discuss cybersecurity and privacy related issues.

(2) Serves as the authorizing body in reviewing, evaluating, and approving enterprise-level cybersecurity documents.

(3) Reviews and approves the Council's charter and subsequent updates.

(4) Provides recommendations regarding cybersecurity and privacy throughout PBGC.

(5) Establishes ad hoc working groups to identify and develop strategic direction and recommendations.

(6) Defines and resolves technical cybersecurity and privacy issues.

p. **Chief Enterprise Architect.**

(1) Works with ECD and OGC to integrate necessary information security, records management, CUI and privacy requirements to ensure organizational mission/business functions are adequately addressed within the enterprise architecture process and procedures (e.g., reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes).

(2) Maintains PBGC's Enterprise Target Architecture (ETA), an authoritative planning document for PBGC functional portfolios and segment architectures.

(3) Describes the activities that guide business units in planning, implementing, and managing their functions to attain the desired target state.

(4) Chairs the PBGC Technology Review Board (TRB) which helps ensure information security, privacy, CUI, and records management issues are addressed in standards and designs.

q. **Procurement Director.**

(1) Ensures that PBGC contracts include appropriate terms and conditions for solicitations and contracts requiring contractors and subcontractors to follow PBGC's policies and procedures for protecting PBGC information.

(2) Enforces terms and conditions of the contract in coordination with requiring activity or program office.

r. **Contracting Officer Representative (COR).**

(1) Notifies the Contracting Officer (CO) in a timely manner if the contractor violates the terms and conditions.

s. **Authorizing Official (AO).**

(1) Assumes responsibility for operating an information system at an acceptable level of risk.

(2) Maintains budgetary oversight for an information system and is responsible for the mission and/or business operations supported by the system.

(3) Approves information security, records management, CUI, and privacy plans, memorandums of agreement or understanding, and determines whether significant changes in the information systems or environments of operation require reauthorization.

t. **Information System User**

(1) Reads, acknowledges, and complies with the requirements of this Directive.

(2) Reads, acknowledges, and complies with the PBGC Rules of Behavior.

(3) Completes annual cybersecurity awareness training and certification requirements as appropriate to this Directive.

(4) As required, completes role-based training specific to his or to her

responsibilities.