Pension Benefit Guaranty Corporation

Directive

Subject: PBGC Information Security Policy

Directive Number: IM 05-02

Originator: OIT

Gordon Hartogensis

Digitally signed by Gordon Hartogensis
Date: 2023.05.08 14:54:39 -04'00'

Gordon Hartogensis
PBGC Director

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

2. **EFFECTIVE DATE**: This Directive replaces PBGC Directive IM 05-02, dated 4/22/2020. 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 14028, "On Improving the Nation's Cybersecurity," (May 12, 2021)
   b. Office of Management and Budget (OMB) Memo 22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022)
   c. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources (1996)
   d. Office of Management and Budget (OMB) Revision Circular A-130, Managing Information as a Strategic Resource (2016)
   e. Office of Management and Budget (OMB) Circular A-11, Preparation, Submission, and Execution of the Budget, §25.5; 51.19
   f. Clinger-Cohen Act of 1996, Public Law 104-106 (40 U.S.C. §1401, et seq.)
   g. Federal Information Security Modernization Act (FISMA) of 2014 (44 U.S.C. §3551, et seq., Public Law (P.L.) 113-283)
   h. The Privacy Act of 1974
   i. Executive Order 13556 Controlled Unclassified Information (Nov. 4, 2010)
   j. Controlled Unclassified Information, 32 CFR Part 2002
   k. Foundations for Evidence-Based Policymaking Act of 2018
   l. Federal Information Processing Standard (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems
   m. FIPS Publication 200, Minimum Security Requirements for Federal

Information and Information Systems

n. FIPS Publication 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors

o. NIST guidance, principally the following NIST special publications:
   (1) NIST SP 800-30, Guide for Conducting Risk Assessments
   (2) NIST SP 800-37, Rev. 2 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, Volume I - Guide for Mapping Types of Information and Information Systems to Security Categories; Volume II - Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices
   (8) NIST 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
   (9) NIST 800-210, General Access Control Guidance for Cloud Systems
   (10) NIST 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

p. PBGC Directive FM 15-03, Suspension and Debarment Program

q. PBGC Directive IM 05-04, Use of Information Technology Resources

r. PBGC Directive IM 05-07, Information Technology Management

s. PBGC Directive IM 05-09, PBGC Privacy Program

t. PBGC Directive IM 10-02, Safeguarding Tax Return Information

u. PBGC Directive IM 10-03, Protecting Sensitive Information

v. PBGC Directive IM 10-05, Media Relations

w. PBGC Directive PM 30-01, Disciplinary and Adverse Actions

x. PBGC Directive IM 15-03, PBGC Records Management Program

y. PBGC Office of Information Technology Glossary of Terms

5. **BACKGROUND**: The PBGC requires that all information systems (regardless of location or delivery mechanism) abide by the 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 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 consequence 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 SecurityRisk: 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 and privacy risks, considering mission priorities, and allocating resources to the most efficient solutions necessary to reduce risk toacceptable levels.
c. Considers the need to synchronize mission execution and performance with business, information technology (IT) infrastructure, and security and privacy requirements.
d. Provides the 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 and privacy.

6. **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 security requirements. The controls establish a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation

within PBGC information systems.

d. **Control Family.** A collection of security and privacy related controls that exhibit a commonality in function or objective, specifically how they protect the confidentiality, integrity, and availability of information or information systems.
e. **Control Parameter.** See Organization-defined control parameter.
f. **Cybersecurity Issuance Document**. Any cybersecurity procedure, guidance, standard, executive memorandum, or bulletin that are collectively referred to as cybersecurity issuance documents.
g. **Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
h. **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.
i. **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 security weaknesses found in programs and systems.
j. **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.
k. **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 security state of the information system.
l. **Rules of Behavior.** Establishes the rules that describe the responsibilities and expected behaviors about information and information system usage.
m. **Security Authorization.** The notice to proceed with the "live" system. It is the official management decision given by a system's Authorizing Official 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 security controls. Security Authorizations are also referred to as an "Authorization to Process (ATP)" or "Authority to Operate(ATO)" or "Authority to Use (ATU)."
n. **System Authorization Boundary.** A description or diagram that includes all components of an information system to be authorized for operation by the authorizing official and excludes separately authorized systems to which the information system is connected.

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

7. **POLICY**: It is PBGC policy to protect its information and information systems in amanner 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, including externally owned and hosted systems in accordance with Federal Information Processing Standard (FIPS) 199, implement a corresponding set of 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) Policy and Process Library (PPL).

c. Address risk management by incorporating 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 Cyber Security Assessment and Management (CSAM) tool as the authoritative source for PBGC information system authorizations and common control programs. All system assessment and authorization artifacts and information shall be stored within CSAM. PBGC's enterprise common controls and organization-defined control parameters shall also be stored within CSAM, and inheritance of common controls shall be documented within the tool.

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

f. Establish a process to deploy privacy and security controls throughout PBGC consistent with the provisions of NIST SP 800 Series, FIPS, other applicable federal mandates, and the PBGC Risk Management Framework (RMF). These processes will facilitate implementation of Directive IM 05-02 and associated controls as described in the NIST SP 800-53 control families table listed below.

g. Comply with standards, organizational defined parameters, procedures, processes, and guidance developed and disseminated by the Enterprise

Cybersecurity Department (ECD) and the Cybersecurity and Privacy Council to address privacy and 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 as described in the NIST Security and Privacy Control Family table as established in NIST 800-53:

NIST Security Control Family
AC - Access Control
AT - Awareness and Training
AU - Audit and Accountability
CA - Security Assessment and Authorization
CM - Configuration Management
CP - Contingency Planning
IA - Identification and Authentication
IR - Incident Response
MA - Maintenance
MP - Media Protection
PE - Physical and Environmental Protection
PL - Planning
PM - Program Management
PS - Personnel Security
PT – PII Processing and Transparency
RA - Risk Assessment
SA - System and Services Acquisition
SC - System and Communications Protection
SI - System and Information Integrity
SR – Supply Chain Risk Management

8. **POLICY DEVIATIONS**:

a. The Chief Information Security Officer (CISO) and Senior Agency Official for Privacy (SAOP) have the authority to approve IT security policy deviations. 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. The 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 deviation requests will be reviewed on an annual basis.

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

e. Any change in the underlying risks that led to the approved policy deviation should be reported to the CISO and/or SAOP as soon as practicable for a determination on whether the approved deviation is still valid and necessary.

f. Policy deviations involving privacy issues must also comply with theprocess set forth in Directive IM 05-09.

9. **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 Security 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) review and action.

10. **PROCESSES**: Cybersecurity documents utilized for implementing privacy and 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 Process and Procedure Library (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 training after cybersecurity documents are published. Cybersecurity documents shall be implemented 180 days after publication.

11. **RESPONSIBILITIES**:

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 Risk Management Officer (RMO) to chair 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 of 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 on 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) Manages 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) 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 as amended, Freedom of Information Act, and PBGC's implementing regulations.
(2) Ensures privacy control requirements are met through the Risk Management Framework (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 informationprivacy 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) Serves as Co-Chair of the PBGC Cybersecurity and Privacy Council.

(10) 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.

f. **Chief Data Officer**

(1) Coordinates with the CISO and the CPO; 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.

g. **Risk Management Officer.**

(1) Encourages PBGC employees to communicate openly and freelyabout current and potential risks to the agency.

(2) Facilitates timely identification of PBGC's risks to help implement mitigation strategies before reaching full impact.

(3) Leads the task of creating an Enterprise Risk Management (ERM) framework to ensure the agency has a consistent risk assessment approach.

h. **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.

i. **Risk Executive (Function).**

(1) PBGC leverages the Risk Management Council along with input from the PBGC CIO, CISO, SAOP to function as the Risk Executive function for the organization.

(2) Through the Risk Management Council, the Risk Executivefunction 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 security authorization actions requiring shared responsibility (e.g., joint/leveraged authorizations).
(k) Ensure that 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.

j. **Cybersecurity and Privacy Council ("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.

k. **Chief Enterprise Architect.**
(1) Works with ECD and OGC to integrate necessary information security 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 and privacy issues are addressed in standards and designs.

l. **Procurement Director.**

(1) Ensures that all contracts and other agreements include provisions requiring contractors and subcontractors to follow PBGC's policies and procedures for protecting PBGC information.

(2) Initiates appropriate corrective action against a contractor for failure to follow PBGC's policies and procedures for protecting PBGC information.

(3) Through Contracting Officers (COs) and Contracting Officer Representatives (CORs), ensures that contractors perform cybersecurity responsibilities in compliance with this Directive.

(4) Ensures that solicitations for IT hardware, software, and professional services have the appropriate references and clauses needed to address information security in the final solicitation package.

m. **Workplace Solutions Department Director.**

(1) Oversees and manages the Workplace Solutions Department, including the Records Management Program and the Homeland Security Presidential Directive (HSPD)-12 program.

(2) Maintains and manages the physical security of PBGC's offices and facilities.

(3) Supports PBGC departments' efforts to ensure that business operations run efficiently, safely, and in compliance with applicable Public Laws, rules, and regulations.

n. **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 security and privacy plans, memorandums of agreement or understanding, and determines whether significant changes in the information systems or environments of operation require reauthorization.

o. **Common Control Provider (CCP).**

(1) Provides management oversight in the development, implementation, assessment, risk management, authorization and monitoring of common controls (i.e., security controls inherited by information systems).

(2) Authorizes approvals and rejections of control requests.

(3) Designates a Point of Contact (POC) to administer Enterprise Common Control (ECC) Change requests and tasks associated with managing common controls under their purview.

(4) Documents the organization-identified common controls in a security plan (or equivalent document prescribed by the organization).

(5) Documents assessment findings in a security assessment report.

(6) Ensures that required assessments of common controls are performed

by qualified assessors with an appropriate level of independence defined by the organization.

(7) Manages the security and privacy common controls they are providing to the agency and the associated organizational-defined control parameters.

(8) Produces POA&Ms or risk acceptances for all controls having weaknesses or deficiencies.

p. **Common Control Provider Point of Contact.**

(1) Manages the administration of offered Common Controls on behalf of the CCP.

(2) Coordinates the development, implementation, assessment, authorization, and monitoring of common controls.

(3) Authorizes approvals and rejections of control requests on behalf of the CCP if needed and supports risk management efforts for common controls.

q. **Information System Security Manager (ISSM).**

(1) Ensures that the operational security posture is managed forinformation systems and programs under their control.

(2) Participates as a member of PBGC Cybersecurity and Privacy Council.

(3) Oversees audits of information systems and security program.

(4) Ensures solicitation requirements for IT hardware, software, and professional services have the appropriate references and clauses needed to address information security and privacy in the final solicitation package.

(5) Ensures the completion of monitoring, testing, and evaluation of the effectiveness of cybersecurity policy, procedures, practices, and security controls are performed and completed with a frequency depending on risk, as directed by ECD.

(6) Contributes information and recommendations to strategic plans and reviews, including preparing and completing action plans, implementing production, productivity, quality, and customer- service standards, resolving problems, completing audits, identifying trends, determining system improvements, implementing any necessary changes to improve system security.

(7) To the extent possible, ensures that costs associated with remediating weaknesses are identified in terms of dollars in CSAM.

r. **Information System Owner (ISO).**

(1) Maintains overall accountability for the procurement, development, integration, modification, or operation and maintenance of an information system.

(2) Addresses the operational interests of the user community (i.e., individuals who depend upon the information system to satisfy mission, business, or operational requirements) and ensures compliance with information security requirements.

(3) Ensures the information system is operated according to the agreed

upon security and privacy requirements.

(4) Manages the system security and privacy controls and associated organizationally defined parameters.

(5) Ensures that adequate security measures and procedures are implemented to protect the data residing on their system(s).

(6) Reviews waiver requests as needed on an annual basis.

(7) Ensures solicitation requirements for IT hardware, software, and professional services have the appropriate references and clauses needed to address information security in the final solicitation package.

s. **Information Owner (IO).**

(1) Establishes policies and procedures governing generation, collection, processing, dissemination, and disposal of information.

(2) Safeguards the information contained in the system he/she owns and retains that responsibility when information is shared with or provided to other organizations.

(3) Ensures that solicitation requirements for IT hardware, software, and professional services have the appropriate references and clauses needed to address information security in the final solicitation package.

t. **Information System Security and Privacy Officer (ISSPO).**

(1) Responsible for ensuring that the security and privacy posture is maintained for an organizational system and works in close collaboration with the system owner.

(2) Serves as a principal advisor on all matters, technical and otherwise, involving the controls for the system.

(3) Has the knowledge and expertise to manage the security or privacy aspects of an organizational system and is assigned responsibility for the day-to-day system security or privacy operations. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security and privacy training and awareness.

(4) Assists in the identification of common controls.

(5) Assists in developing and updating the System Security Plan (SSP), and coordinating with the IO/ISO, any changes to the information system and assesses the security impact of those changes.

(6) Ensures systems are operated, maintained, and disposed of in accordance with policies outlined in the approved security authorization package.

(7) Reports all incidents.

(8) Maintains, reviews, and updates interconnection security agreements (ISA) at least annually and as required by terms of the ISA.

u. **Security Control Assessor (SCA).**

(1) An individual, group, or organization responsible for conducting a comprehensive assessment of implemented controls and control enhancements to determine the effectiveness of the controls (i.e. the extent to which the controls are implemented correctly, operating as

intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization).

(2) Prior to initiating the control assessment, the assessor reviews the security and privacy plans to facilitate development of the assessment plan.

(3) Provides an assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls and can recommend corrective actions to address the identified vulnerabilities.

(4) Prepares security and privacy assessment reports containing the results and findings from the assessment.

v. **System Security and Privacy Engineer.**

(1) An individual, group, or organization responsible for conducting systems security or privacy engineering activities as part of the System Development Life Cycle (SDLC). System security and privacy engineering are processes that capture and refine security and privacy requirements for systems and ensure that the requirements are effectively integrated into systems and system elements through security or privacy architecture, design, development, and configuration.

(2) Participates as part of the development team -- designing and developing organizational systems or upgrading existing systems along with ensuring that continuous monitoring requirements are addressed at the system level.

(3) Employs best practices when implementing controls including software engineering methodologies, system and security or privacy engineering principles, secure or privacy-enhancing design, secure or privacy-enhancing architecture, and secure or privacy-enhancing coding techniques.

(4) Coordinates security and privacy activities with senior agency information security officers, senior agency officials for privacy, security and privacy architects, system owners, common control providers, and system security or privacy officers.

w. **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 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.