



# Order

---

**Subject:** PBGC Information Security Policy

---

**Directive Number:** IM 05-2

**Effective Date:** 03/23/12      **Originator:** OIT

Alice C. Maroni  
Chief Management Officer

---

1. **PURPOSE:** This Order establishes the Pension Benefit Guaranty Corporation's (PBGC) Information Security Policy and outlines the PBGC security policy guidance provided by the National Institute of Standards Technology (NIST), in Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.
2. **CANCELLATION:** This Order replaces the policy portions of PBGC Directive IM 05-2, Information Assurance Handbook (IAH), dated 7/23/2008 ("Section I" of each Volume identified within the IAH). The procedures within PBGC Directive IM 05-2 ("Section II" of each Volume) remain in effect until specifically replaced by an Office of Information Technology (OIT) Standard, Process, Procedure, or Guideline. On March 27, 2015, administrative changes were made relating to the delegation of the PBGC Director's duties in the event of the PBGC Director's absence.
3. **SCOPE:** This Order applies to all information systems operated by or on behalf of the PBGC. Exceptions to these Information Security Policies or Standards shall be requested through the PBGC's Enterprise Information Security Office (EISO).
4. **AUTHORITIES:**
  - a. Clinger-Cohen Act of 1996, Law 104-106 (40 U.S.C. §1401, *et seq.*)
  - b. Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. §3541, *et seq.*)
  - c. Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
  - d. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
  - e. FIPS Publication 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*

- f. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- g. OMB Circular A-130, *Management of Federal Information Resources*, Appendix III: Security of Federal Automated Information Resources
- h. OMB Circular A-11, *Preparation, Submission, and Execution of the Budget*, §25.5; 51.18 (Budgeting for the Acquisition of Capital Assets)
- i. NIST guidance, principally the following NIST special publications:
  - (1) NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems
  - (2) NIST SP 800-30, Guide for Conducting Risk Assessments
  - (3) NIST SP 800-37, Guide to Applying the Risk Management Framework to Federal Information Systems: *A Life Cycle Approach*
  - (4) NIST SP 800-39, Managing Information Security Risk: *Organization, Mission, and Information System View*
  - (5) NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations
  - (6) NIST SP 800-60, Volume I - Guide for Mapping Types of Information and Information Systems to Security Categories; Volume II – Appendices to the Guide for Mapping Types of Information and Information Systems to Security Categories

5. **BACKGROUND:** The PBGC requires that all information systems (regardless of location or delivery mechanism) abide by the security policies set forth in this Order in order to ensure the confidentiality, integrity and availability of data in PBGC information systems.

The Federal Government has instituted a number of 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.

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 around the control families defined in *NIST SP 800-53, Security Controls for Federal Information Systems and Organizations*.

6. **DEFINITIONS:** For the purpose of this directive, the following definitions apply.
- a. **Authority to Operate (ATO)** – The notice to proceed with the “live” system. It is the official management decision given by a senior PBGC official to authorize operation of an information system and to explicitly accept 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. ATO is also referred to as an “Authorization to Process” or “Accreditation.”
  - b. **Baseline Configuration** – Information about the components of an information system, network topology, and the logical placement of the component within the system architecture. A baseline configuration is a documented, up-to-date specification to which the information system is built.
  - c. **Common Control** – Common controls are security controls that are inheritable by one or more organizational information systems. The organization assigns responsibility for common controls to appropriate organizational officials and coordinates the development, implementation, assessment, authorization, and monitoring of the controls.
  - d. **Computer Emergency Response Team (CERT)** – The name given to expert groups that handle computer security incidents.
  - e. **Control Family** – A collection of security related controls that exhibit a commonality in function or objective, specifically how they protect the confidentiality, integrity and availability of information or information systems.
  - f. **Critical Infrastructure** – The systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on all aspects of national security, national public health and safety, or any combination of those matters.
  - g. **Controlled Unclassified Information (CUI)** – A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but (i) is pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) which law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces Sensitive But Unclassified (SBU).
  - h. **Enterprise Architecture** – A strategic information asset base that defines business mission needs, the information content necessary to operate the business, the information technologies necessary to support business operations, and the transitional processes necessary for implementing new technologies in response to changing business mission needs. Enterprise architecture includes baseline architecture, target architecture and a sequencing plan.
  - i. **Incident** – An event that results in a breach of the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system.

- j. **Information System** – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. The Federal Information Security Management Act (FISMA) emphasizes the need for each federal agency to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
- k. **Interconnection Security Agreement (ISA)** – A security document that specifies the technical and security requirements for establishing, operating, and maintaining the interconnection. Specifically, the ISA documents the requirements for connecting the IT systems, describes the security controls that will be used to protect the systems and data, contains a topological drawing of the interconnection, and provides a signature line.
- l. **Management Controls** – The security controls (i.e., safeguards or countermeasures) for an information system that are focused on the management of risk and information system security.
- m. **Operational Controls** – The security controls (i.e., safeguards or countermeasures) for an information system that are implemented and executed by people (as opposed to systems).
- n. **PBGC Contractor** – For purposes of this Order, PBGC contractors include any individual providing services to PBGC under contract or purchase order or any individual who is an employee of a firm or entity that provides services to the PBGC under a contract or purchase order.
- o. **PBGC Employee** – For purposes of this Order, PBGC employees include any full-time, temporary employee on detail, stay-in-school staff, and interns.
- p. **Plan of Action and Milestones (POA&M)** – A management process that outlines weaknesses and delineates the tasks necessary to mitigate them. The PBGC Information Security Program POA&M process is used to facilitate the remediation of information security program- and system-level weaknesses, and provides a means for planning and monitoring corrective actions, defining roles and responsibilities for weakness resolution, assisting in identifying the information security funding requirements necessary to mitigate weaknesses, tracking and prioritizing resources, identifying those risks deemed acceptable that will not be mitigated, and informing decision makers.
- q. **Privacy Impact Assessment (PIA)** – An analysis of how information is handled: (i) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
- r. **Personally Identifiable Information (PII)** – Information that can be used to identify, contact, or locate a single person, or that can be used with other sources to identify a single individual.

- s. **Privacy Threshold Analysis (PTA)** – A prerequisite to the PIA that determines if PII data will exist in the information system identified and whether a PIA will be required.
- t. **Program Management Controls** – Those controls that focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security.
- u. **Risk Assessment** – The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls that are planned or already in place.
- v. **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.
- w. **Rules of Behavior** – Establishes the rules that describe the responsibilities and expected behaviors with regard to information and information system usage.
- x. **System Authorization Boundary** – A description or diagram that includes all components of an information system to be authorized for operation (by an authorizing official), and excludes separately authorized systems to which the information system is connected.
- y. **System Security Plan (SSP)** – A plan that details the types of security required for a security solution based on the type of information being processed and the degree of sensitivity. The SSP also identifies whether the PBGC Security Office requires that the system be certified and accredited.
- z. **System of Records** – A group of any records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other unique identifier assigned to the individual.
- aa. **System of Record Notice (SORN)** – A notice published by an agency in the Federal Register to provide public notice of the data contained in a system of records that the agency has organized and how the collected information is used.
- bb. **Technical Controls** –The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
- cc. **Weakness** – A system security vulnerability that has been identified by any party’s assessment of the security of a system.

## 7. **POLICIES:**

The following policies are derived from, and embodied by, the PBGC Information Security Standards and Information Security Controls Matrix. They are based on NIST SP 800-53 and are classified into four security control categories: Management, Operational, Technical, and Program Management controls. These policies are supported by OIT standards, processes, procedures and guidelines. They are, reviewed and approved by the OIT Governance Boards, which 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.

NOTE: As stated above, parameters of these policies (e.g. frequency, format, etc.) are contained in individual Security Standards related to these Management, Operational and Technical controls.

### a. **Management Controls**

The following Management Controls focus on the management of risk and information system security.

#### (1) **Risk Assessment (RA Control Family)**

- a. All systems shall undergo periodic security categorization in accordance with FIPS 199 and FIPS 200, which will determine the required security controls for that system.
- b. All systems shall undergo periodic Risk Assessments to identify likely vulnerabilities, threats and threat sources, and to determine residual risks based on planned and known control effectiveness.
- c. All systems shall undergo periodic vulnerability scans.

#### (2) **Planning (PL Control Family)**

- a. Privacy Impact Assessments (PIA) shall be prepared for all required systems and reviewed periodically.
- b. System Security Plans (SSP) shall be prepared and maintained for all systems and reviewed periodically.
- c. Enterprise Rules of Behavior (RoB) shall be developed to cover all systems.
- d. These documents (PIA, SSP, RoB and other supporting security documentation) shall be available to the Senior Agency Information Security Officer (SAISO) for compliance oversight.

**(3) Security Assessment and Authorization (CA Control Family)**

- a. System authorization boundaries of all PBGC information systems shall be defined and documented, including minor applications contained within a system.
- b. External systems that are directly interconnected with PBGC networks or systems shall be documented in an Interconnection Security Agreement (ISA). All external systems to which PBGC information systems are connected shall be protected by the same or comparable security controls and have an “Authority to Operate” in accordance with federal certification and accreditation guidelines.
- c. All information systems operated by or on behalf of PBGC are required to be documented, independently assessed for security compliance, and authorized by the Authorizing Official (AO).
- d. Ongoing continuous monitoring of controls shall be planned and executed accordingly to identify risks.
- e. All weaknesses, regardless of identification source (e.g., internal audits, Inspector General (IG) audits, Government Accountability Office (GAO) audits, etc.), shall be maintained in a Plan of Action and Milestones (POA&M) until resolved.

**(4) System and Services Acquisitions (SA Control Family)**

- a. Sufficient security resources shall be allocated to protect information systems. Necessary security resources shall be reflected in capital planning efforts.
- b. System development life cycle processes shall incorporate information security considerations.
- c. System service and system development contracts shall include security clauses and language detailing system security requirements, as appropriate.

**b. Operational Controls**

The following Operational Controls focus on controls primarily managed by people (as opposed to being managed by systems).

**(1) Awareness and Training (AT Control Family)**

- a. General security awareness training shall be provided periodically to all users.
- b. Role-based annual training shall be provided to those users with substantial security responsibilities.

- (2) **Configuration Management (CM Control Family)**
  - a. PBGC (typically owners or collaborators) shall develop and maintain information system security and component inventories, including hardware, software, and firmware.
  - b. Information systems shall conform to established baseline configurations.
  - c. Appropriate configuration change control processes shall be established and followed to ensure that PBGC information system configuration changes are controlled properly, documented, and that documentation is retained and reviewed.
  
- (3) **Contingency Planning (CP Control Family)**
  - a. Contingency and recovery plans shall be developed and maintained for PBGC information systems.
  - b. Recovery plans shall be distributed, shared, and tested.
  
- (4) **Incident Response and Management (IR Control Family)**
  - a. An operational incident response plan and handling capability shall be maintained for operational systems and include personnel training.
  - b. Security incidents shall be tracked, documented, and reported as appropriate.
  
- (5) **Maintenance (MA Control Family)**
  - a. Appropriate resources (plans, schedules, tools and personnel) shall be identified to ensure the timely maintenance of information system hardware and software.
  
- (6) **Media Protection (MP Control Family)**
  - a. Protections to information system media (both paper and digital) to protect the media from loss, alteration, or theft shall be provided.
  - b. Access to the information and the information system shall be limited to authorized users.
  - c. Media shall be sanitized or destroyed before it is repurposed or disposed of.
  
- (7) **Physical and Environmental Protection (PE Control Family)**
  - a. Physical access to information systems, equipment, and operating environments shall be limited to authorized personnel.
  - b. Assets shall be protected against unauthorized use, theft, environmental hazards, or inadvertent destruction.

(8) **Personnel Security (PS Control Family)**

- a. PBGC shall apply controls to ensure personnel (federal and contractor) are trustworthy and meet established security criteria for the positions personnel occupy.
- b. Physical and logical access of employees and contractors who separate from PBGC shall be terminated promptly.
- c. Formal sanctions shall exist for personnel failing to comply with PBGC security policies and procedures.

(9) **System and Information Integrity (SI Control Family)**

- a. The Information System Owner (ISO), Information System Security Officer (ISSO), and technical support staff shall employ processes to identify, report, and correct information and information system flaws in a timely manner.
- b. Controls shall be in place to protect information systems from malicious code and other vulnerabilities.

c. **Technical Controls**

Technical controls 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.

(1) **Access Control (AC Control Family)**

- a. Information systems shall employ methods to identify and authenticate users, devices and processes.
- b. Access shall be granted to, and removed from, users and/or user groups as appropriate.
- c. Controls appropriate to the mode of connection (e.g., wireless, remote, etc.) shall be in place on information systems.

(2) **Audit and Accountability (AU Control Family)**

- a. Systems shall produce audit trails for all significant activities.
- b. Agency processes shall support audit trail reviews to enable identification of, and responses to, suspicious activities.

(3) **Identification and Authentication (IA Control Family)**

- a. Users, processes, and devices shall be properly identified and authenticated before being connected to system resources.

(4) **System and Communications Protection (SC Control Family)**

- a. Agency communications shall be monitored, controlled, and protected at the external perimeter and key internal boundaries of systems.
- b. Systems shall be built on the basis of architectural design, software development techniques, and engineering principles that promote effective information security (e.g., partitioning, isolation, shared resources, etc.).

d. **Program Management Controls**

Program Management controls are those controls that are not system specific but provide agency-wide information security assurance.

(1) **Information Security Program Plan (PM-1)**

PBGC shall maintain an Information Security Program plan that:

- a. Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
- b. Provides sufficient information about the program management controls and common controls to enable an implementation that is unambiguously compliant with the intent of the plan, and a determination of the risk to be incurred if the plan is implemented as intended.
- c. Includes roles, responsibilities, management commitment, coordination among PBGC entities, and compliance.
- d. Is approved by the CIO.

(2) **Senior Agency Information Security Officer (PM-2)**

PBGC shall maintain the position of SAISO within the OIT with the mission and resources to coordinate, develop, implement, and maintain an agency-wide information security program.

(3) **Information Security Resources (PM-3)**

Through the Capital Planning and Investment Program, PBGC shall ensure that all capital planning and investment requests provide for the resources needed to implement the information security program, and that all exceptions to this requirement are documented, including the employment of a business case/Exhibit 300/Exhibit 53 to record the resources required. This will ensure that information security resources are available for expenditures as planned.

(4) **Plan of Action and Milestones Process (PM-4)**

PBGC shall implement and maintain a POA&M process for ensuring that the security program, and the associated PBGC information systems document and monitor the remedial information security actions that will mitigate risk to agency operations and assets, individuals, other organizations and the Nation.

(5) **Information System Inventory (PM-5)**

Through registration and decommission processes, PBGC shall develop and maintain an inventory of its information systems.

(6) **Information Security Measures of Performance (PM-6)**

As part of the Information Security Program plan, PBGC shall develop, monitor, and report the results of information security measures of performance.

(7) **Enterprise Architecture (PM-7)**

As part of the Enterprise Architecture Program Management plan, PBGC shall develop an enterprise architecture with consideration for information security and for the resulting risk to agency operations and assets, individuals, other organizations, and the Nation.

(8) **Critical Infrastructure Plan (PM-8)**

PBGC is not part of the government's critical infrastructure. This control is, therefore, not applicable to the PBGC.

(9) **Risk Management Strategy (PM-9)**

Through the PBGC OIT Risk Management process and the PBGC Information Security Program plan, PBGC shall develop a comprehensive strategy to manage the risk to agency operations and assets, individuals, other organizations, and the Nation where risk is associated with the operation and use of information systems, and shall implement that strategy consistently across the agency.

(10) **Security Authorization Process (PM-10)**

PBGC shall develop and maintain a Security Assessment and Authorization process that (a) manages (i.e., documents, tracks, and reports) the security state of agency information systems through security authorization processes, (b) designates individuals to fulfill specific roles and responsibilities within the PBGC risk management process, and (c) fully integrates the security authorization processes into an agency-wide risk management program.

(11) **Mission and Business Process Definitions (PM-11)**

Through OIT program plans, policies, procedures, guides and standards, OIT shall define mission and business processes with consideration of information security and the resulting risk to PBGC operations and assets, individuals, other organizations, and the Nation; shall determine information protection needs arising from the defined mission and business processes; and shall revise the processes as necessary until said protection needs are satisfied.

## 8. ROLES and RESPONSIBILITIES:

The following are the roles and responsibilities that are essential to delivering secure systems at PBGC. These roles are generally defined in NIST SP 800-37.

### a. **PBGC Director, or in the absence of the PBGC Director, the Chief Information Officer**

1. Has the overall responsibility to provide information security protections commensurate with the risk and impact of harm to the PBGC's operations, assets, and individuals.
2. Ensures development and implementation of strong 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 being carried out by PBGC.

### b. **Risk Executive (function)**

The Risk Executive function is supported by individuals or groups that help to ensure: (i) risk-related considerations for individual information systems, including but not limited to authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

### c. **Chief Information Officer**

1. Designates a Senior Agency Information Security Officer (SAISO).
2. Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements.
3. Establishes the Risk Executive function with approval of PBGC's Executive Management Committee.
4. Oversees personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained.
5. Assists senior [organizational] officials concerning their security responsibilities.
6. Coordinates with other senior officials, reporting periodically to the Agency Director on the overall effectiveness of the agency's information security program, including the progress of remedial actions.
7. Evaluates and approves the designation of Authorizing Officials (AO).
8. Designates common controls.

The CIO, with the support of the SAISO, works closely with AOs and their designated representatives to help ensure that:

1. An agency-wide information security program is effectively implemented resulting in adequate security for all PBGC information systems and operational environments for those systems;
2. Information security considerations are integrated into programming, planning and budgeting cycles, enterprise architectures, and acquisition and system development life cycles;
3. Information systems are covered by approved security plans and are authorized to operate;
4. Information security-related activities required across the agency are accomplished in an efficient, cost-effective, consistent, and timely manner; and
5. There is centralized reporting of appropriate information security-related activities to the appropriate agency officials.

d. **Executive Management Committee**

Approves the implementation of the Risk Executive function.

e. **Chief Architect**

The Chief Architect works closely with the program managers, the Senior Agency Information Security Officer (SAISO), and the business owners to ensure that all technical architecture requirements are adequately addressed in the application of the Federal Enterprise Architecture (FEA) and the Security and Privacy Profile (SPP).

f. **Senior Agency Information Security Officer**

1. Carries out the CIO security responsibilities under Federal Information Security Management Act (FISMA).
2. Serves as the primary liaison for the CIO to the agency's authorizing officials, information system owners, common control providers, and information system security officers.
3. Possesses professional qualifications, including training and experience, required to administer the information security program functions.
4. Maintains information security duties as a primary responsibility.
5. Heads an office with the mission and resources to assist the agency in achieving more secure information and information systems in accordance with the FISMA requirements.
6. Maintains Information Security-related documents including policies, procedures, standards, guides, templates, and other tools (including the Information Security Program plan).
7. Designates Information System Security Officers (ISSO).
8. Ensures the consistency and quality of authorization packages submitted for AO review.

9. Oversees the PBGC-wide POA&M process.
10. Oversee FISMA reporting.
11. Concurs on information system categorizations.
12. Ensures the assessment, updating, and dissemination of information regarding PBGC Common Controls.
13. Oversees security awareness and training for agency and contractor personnel.

The role of the SAISO has inherent U.S. government authority and shall be assigned to government personnel only.

**g. Authorizing Official**

Authorizing Officials (AO) are department directors or Senior Level (SL) officials with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, assets, and individuals. AOs typically have budgetary oversight for an information system or are responsible for the mission and/or business operations supported by the system. Through the security authorization process, AOs are accountable for the security risks associated with information system operations. Accordingly, AOs are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. AOs also:

1. Approve security plans and POA&Ms and determine, in coordination with the SAISO, whether significant changes in the information systems or operational environments require reauthorization.
2. Deny, as appropriate, authorization to operate an information system or, if the system is operational, halt operations if unacceptable risks exist.
3. Coordinate their activities with the CIO, SAISO, common control providers, Information System Owners (ISO), ISSOs, security control assessors, and other interested parties during the security authorization process.
4. Allocate sufficient resources to adequately protect information and information systems based on an assessment of agency risks.
5. Ensure that security control assessors of the AO's systems have a sufficient level of independence.
6. Approve PIAs for the information system.
7. Coordinate with OGC to ensure appropriate SORNs are in place.

**h. Common Control Provider**

Common Control Providers are individuals, groups, or organizations that are responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). Common control providers:

1. Document the agency-identified common controls in a SSP (or equivalent document prescribed by the agency).

2. Ensure that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the agency.
3. Document assessment findings in a security assessment report.
4. Produce POA&Ms for all controls having weaknesses or deficiencies and ensure that security plans, security assessment reports, and POA&Ms for common controls (or summaries of such information) are made available to ISOs whose systems have inherited those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.
5. Support ISOs and others in the understanding and implementation of the common controls, and in the building of SSPs.
6. Participate, as required, in audits and assessments of systems inheriting their common controls.

i. **Information Owner**

Information Owners (IO) are PBGC employees with statutory, management, or operational authority for specified information. The IOs:

1. Oversee established policies and procedures governing its generation, collection, processing, dissemination, and disposal.
2. Establish the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. (The owner of the information processed, stored, or transmitted by the information system may or may not be the same person as the system owner, and a single information system may contain information from multiple information owners.)
3. Provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.
4. Assess information for privacy impact and create a PIA based on the assessment.

j. **Information System Owner**

Information System Owners (ISO) are agency employees who are each responsible for and associated with the procurement, development, integration, modification, operation, maintenance, and disposal of an information system. The ISOs also:

1. Ensure information system compliance with information security requirements.
2. Ensure the development, maintenance, and availability of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls.
3. Decide who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

4. Receive the security assessment results from the security control assessor. After taking appropriate steps to reduce or eliminate vulnerabilities, the ISO assembles the authorization package and submits the package to the AO for approval or denial.
5. Ensure funding requests for information security requirements are included in annual budget submissions.
6. Utilize, to the extent possible, agency- provided resources (including infrastructure assets).
7. Develop ISAs for their information systems, as applicable.
8. Ensure capabilities to continuously monitor the security posture of their information systems.
9. Ensure the creation and completion of POA&Ms or provide documented acceptance of risk.
10. Assess information systems for privacy impact and create a PIA based on the assessment.

**k. Information System Security Officer**

Information System Security Officers (ISSO) are individuals who are each responsible for ensuring that the appropriate operational security posture is maintained for an information system and who, as such, work in close collaboration with the respective ISO of the respective system. The ISSOs:

1. Serve as a principal advisor on all matters, technical and otherwise, involving the security of an information system.
2. Maintain detailed knowledge and expertise required to manage the security aspects of an information system and shall be assigned responsibility for the day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protections, personnel security, incident handling, and promoting security training and awareness.
3. Assist in the development of the security policies and procedures and ensures compliance with those policies and procedures.
4. Report, in close coordination with the ISO, to the Enterprise Information Security Office (EISO) and have an active role in the monitoring of a system and its operational environment, to include developing and updating the security artifacts, managing and controlling changes to the system, assessing the security impact of those changes, and participating in audits of the system.
5. Maintain POA&Ms and assist in the remediation of identified weaknesses.
6. Support the PBGC's Computer Emergency Response Team (CERT) in maintaining situational awareness and readiness for potential threats and responses.
7. Ensure Security Control Assessor personnel have sufficient qualifications.

l. **Security Control Assessor**

Security Control Assessors (SCA) are individuals or teams responsible for conducting a comprehensive assessment of the managerial, operational, and technical security controls employed within, or inherited by, an information system in order to determine the overall 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 requirements for the system). Security control assessors also:

1. Provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its operational environment and recommend corrective actions to address identified vulnerabilities.
2. Prepare the final security assessment report containing the results and findings from the assessment. The required level of assessor independence is determined by the specific conditions of the security control assessment and is approved by the system's AO and the SAISO.

m. **Chief Privacy Officer**

The Chief Privacy Officer's role is defined in PBGC Directive IM 05-9, Information Privacy Program. The Chief Privacy Officer:

1. Assists in the development of PBGC's privacy and data protection policies and procedures.
2. Develops, and provides guidance to ISOs on conducting, Privacy Impact Assessments (PIAs) and on drafting System Of Record Notices (SORNs).
3. Coordinates the review and completion of PIAs and SORNs for PBGC information systems.

n. **Information System Security Engineer**

The Information System Security Engineer (ISSE) is responsible for conducting information system security engineering activities.