



Order

Subject: Information Assurance Handbook (IAH)

Directive Number: IM 05-2

Effective Date: 7/23/08 Originator: OIT

Chief Management Officer

1. **PURPOSE:** This directive establishes PBGC Information Technology (IT) security policies, and procedures.
2. **CANCELLATION:** This replaces the May 31st, 2007 version of the Information Assurance Handbook (IAH).
3. **SCOPE:** The policies and procedures contained within are designed to ensure that all information systems operated by or on behalf of the PBGC or under development meet the confidentiality, integrity, and availability commensurate with the sensitivity of the information they process, transmit or store as defined by Federal statutes, regulations, and directives.
4. **AUTHORITY:**
 - (a) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002
 - (b) Federal Records Act of 1950 as Amended, 44 U.S.C. § 3101 et seq.
 - (c) Federal Records Act of 1950 as Amended, 44 U.S.C. § 3301 et seq.
 - (d) Fraud and Related Activities in Connection with Computers, 18 U.S.C. 1030
 - (e) Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, November 28, 2000.
 - (f) Office of Management and Budget Memorandum M-04-04, E-Authentication Guidance for Federal Agencies
 - (g) Office of Management and Budget Memorandum 01-05, “*Guidance on Inter-Agency Sharing of Personal Data*” – *Protecting Personal Privacy*, December 20, 2000.

- (h) Office of Management and Budget Memorandum 03-22, “*Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*”, September 30, 2003.
- (i) Office of Management and Budget Memorandum 06-16, “*Protection of Sensitive Agency Information*”, June 23, 2006
- (j) Office of Management and Budget Memorandum M-99-20, Security of Federal Automated Information Resources
- (k) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994
- (l) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974
- (m) Part 1 of Executive Order 12674, *Implementing Standards of Ethical Conduct for Employees of the Executive Branch*
- (n) Homeland Security Presidential Directive / HSPD-7, December 17, 2003
- (o) Presidential Decision Directive 67, *Continuity of Operations*, October 21, 1998.
- (p) FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
- (q) FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
- (r) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.
- (s) National Institute of Standards and Technology (NIST) Guidance
- (t) PBGC Directive IM 05-04, *Use of Information Technology Resource Policy*

5. **BACKGROUND:** The United States (U.S.) Congress and the Office of Management and Budget (OMB) have instituted a number of laws, regulations, and directives that govern 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 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 the agency head to IT users.

The PBGC’s Information Assurance Handbook (IAH) is 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. The IAH is organized by the seventeen security families identified by NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems. Each of the seventeen security families is presented in a stand-alone volume with each volume presenting the background, purpose, scope and applicability, and authority for the specific family. The volumes are further subdivided into two sections. Section I contains the policies and roles and responsibilities. Section II contains the procedures guidelines, and templates.

6. **DEFINITIONS:**

- (a) **Volume Number and Title:** Describes the formal number of the volume - Identification name assigned to the policy

- (b) **Background:** Provides overview of Federal requirements for the policy.
- (c) **Purpose:** Provides a statement summarizing the objective of the policy.
- (d) **Scope & Applicability:** Provides specification to the extent the policy applies.
- (e) **Authority & Reference:** Enumerates the Federal laws, regulations, standards, and other authoritative requirements from which the policy is derived.
- (f) **Policy:** Statements of the PBGC'S rules and regulations that govern the particular subject matter of the volumes.
- (g) **Roles and Responsibilities:** Identifies positions within PBGC and designation by Federal mandates to ensure policy compliance.
- (h) **Compliance:** Establishes expectation for policy observance.

POLICY: See link -- <http://intranet/dirpoldel/iah.cfm>

7. **RESPONSIBILITIES (Roles):** Everyone within PBGC has a role in maintaining the security of its information resources. For assigning security responsibilities, some executive roles have been defined. Each policy specifies the particular responsibilities that are assigned to each of these roles as applicable. Individuals may serve in multiple roles for different aspects of their jobs. For example, a business unit Manager may serve as an Information System Owner for a particular resource and as a Manager for the employees in his/her department. The roles specified in the PBGC's information security policies are defined as follows:

Chief Information Officer (CIO)

The Chief Information Officer has the following responsibilities with respect to Security Planning:

- Designates a Senior Agency Information Security Officer who shall carry out the CIO's responsibilities for System Security Planning.
- Develops, maintains, and facilitates the implementation of a sound and integrated information technology architecture for the agency.
- Promotes the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

General Counsel

The General Counsel has the following responsibilities with respect to personnel security:

- Ensures consistent and appropriate sanctions for personnel violating management operation, or technical information security controls.

Chief Enterprise Architect (CEA)

The Chief Enterprise Architect has the following responsibilities with respect to media protection:

- Leads PBGC enterprise architecture development and implementation efforts
- Collaborates with lines of business within PBGC to ensure proper integration of lines of business into enterprise architecture
- Participates in PBGC strategic planning and performance planning activities to ensure proper integration of enterprise architecture
- Facilitates integration of information security into all layers of enterprise architecture to ensure agency implementation of secure solutions
- Develops, maintains, and facilitates the implementation of a sound and integrated information technology architecture for the agency
- Promotes the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency

Senior Agency Information Security Officer (SAISO)

The Senior Agency Information Security Officer has the following responsibilities with respect to Security Planning:

- Carries out the CIO's responsibilities for System Security Planning.
- Develops and maintains information security policies, procedures, and control techniques to address System Security Planning.
- Manages the identification, implementation, and assessment of common security controls for the PBGC and documents the results in PBGC's common controls system security plan.
- Performs oversight of department compliance with PBGC's information security policies and procedures.
- Coordinates the identification, implementation, and assessment of the common security controls.

Senior Agency Official for Privacy (SAOP)

The Senior Agency Official for Privacy has the following responsibilities with respect to PIA:

- Responsible for directing the overall implementation of the Privacy Act and privacy policy for PBGC.
- Field questions that departments have about privacy arising from the completion of the PIA and can answer questions about the implications of the personal information contained within their systems.
- Review all completed PIAs.
- Assist departments with publication of system of record notice (SORN) in the Federal Register.

Designated Approving Authority (DAA)

The Designated Approving Authority has the following responsibilities with respect to Security Planning:

- Approves system security plans as part of the certification and accreditation process (C&A).
- Authorizes operation of an information system.
- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.
- Designates the Information System Owner.

Information System Security Officer (ISSO)

The Information System Security Officer has the following responsibilities with respect to Security Planning:

- Implements the common and specific security controls identified by SAISO.
- Plays an active role in coordinating the development and update of the system security plan as well as coordinating with the Information System Owner any changes to the system and assessing the security impact of those changes.
- Assisting with the development and review of system security plans.
- Auditing systems to ensure that their security plans have been effectively implemented.

Information System Owner (ISO)

The Information System Owner or Information System Owner Designee (designated in writing) has the following responsibilities with respect to Security Planning:

- Develops the SSP in coordination with the SAISO, ISSO, and functional end users.
- Maintains the SSP and ensures that the system is deployed and operated according to the security requirements approved by the DAA.
- Establishes the rules of behavior for the information system.
- Authorizes access and the types of privileges or access rights to the information system.
- Authorizes minor changes to the security controls provided there is not an increase in risk to the information system.
- Updates the system security plan whenever a significant change occurs or every three years at a minimum.
- Assists in the implementation of the common and specific security controls.

Director of Facilities and Services Department (FASD)

The Director of FASD is responsible for the following with respect to Physical and Environmental Protection:

- Ensures the implementation of the physical and environmental protection security controls.

Personnel Security Officer

The personnel security Officer has the responsibilities with the respect to the Personnel Security:

- Develops, promulgates, implements, and monitors the organization's personnel security programs.

- Initiates and adjudicates all background investigations for all PBGC Federal and contract personnel.
- Provides guidance to PBGC contracting Officer's Technical Representatives (COTR).
- Develops and implements position categorization (including third-party controls access agreements and personnel screening, termination, and transfers).
- Ensures consistent and appropriate sanctions for personnel violating management operation, or technical information security controls

Configuration Manager

The Configuration Manager has the responsibility of:

- Developing, implementing, and maintaining configuration management procedures.
- Working with Information System Owners to ensure that configuration management policies and procedures are followed and documented.
- Monitoring PBGC information systems to ensure compliance with this policy.
- Documenting, implementing and maintaining the configuration management plan.
- Establishing system baselines and evaluating controls
- Ensuring existence of a process for storing, retrieving and distributing CM materials

Change Manager

The Change Manager has the responsibility of:

- Developing, implementing, and maintaining change management procedures.
- Working with Information System Owners to ensure that change management policies and procedures are followed and documented.
- Monitoring PBGC information systems to ensure compliance with this policy.
- Ensuring that proposed changes do not adversely affect agency systems or data;
- Managing change requests and coordinating implementation of changes;
- Conducting impact analysis of changes;
- Approving, denying, or deferring changes;
- Notifying users of system changes
- Ensuring that an audit trail of changes is documented and maintained.

Contingency Plan Coordinator (CPC)

The Contingency Plan Coordinator has the following responsibilities with respect to Contingency Planning:

- Responsible for monitoring the development of the contingency plan, conducting training and awareness, and performing contingency plan testing;
- Responsible for designating appropriate teams to implement the strategy.
- Responsible for coordinating strategy development with contingency workgroups, team leads, business process owners, and management;
- Routinely update the plan documentation to ensure all information is kept current;

- May appoint a facilitator to assist with coordination, consolidation, and maintenance of the contingency plan; and
- Ensures that reviews are completed in a timely manner.

Project Manager (PM)

The Project Manager has the following responsibilities with respect to system and services acquisition:

- Conducts requirements analysis and alternative analysis.
- Develop major investment supporting materials and IT Initiative Concept;
- Approve integrated project team membership.
- Prepare investment review submission package.
- Maintain cost, schedule, and technical performance baseline.
- Provide Department and agency level managers' visibility into project performance.
- Identify, assess, mitigate, and manage risk;
- Establish management controls and ensure IT security and privacy controls are in place.
- Initiate and continue to refine the project business case.
- Implement and continue to refine the project EVM system.
- Measure variances and quantify trends.

Network Administrator

The Network Administrator has the following responsibilities with respect to System and Information Integrity:

- Installing and configuring hosts in compliance with the PBGC security policies and standard system/network configurations.
- Maintaining hosts in a secure manner, including frequent backups and timely application of patches.
- Monitoring system integrity, protection levels, and security-related events
- Following up on detected security anomalies associated with their information system resources.
- Conducting security tests as required.

User Representatives

The User Representatives have the following responsibilities with respect to System and Information Integrity:

- Represent the operational interests of the user community and serve as liaisons for that community throughout the ITSLCM of the information system.

Information System User (ISU)

The Information System User has the responsibility to comply with the policies and procedures set forth by this Order.

Certification Agent (CA)

The Certification Agent is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome. The Certification Agent must be independent from those individuals responsible for correcting security deficiencies identified during the certification process. The Certification Agent has the following responsibilities with respect to certification and accreditation:

- Coordinates and oversees assessment/testing activities.
- Recommends corrective actions to reduce or eliminate identified vulnerabilities to the information system.
- Provides an independent assessment of the system security plan to ensure the selected security controls are adequate to meet all applicable security requirements.
- Performs an independent security control assessment to ensure that the selected controls are properly implemented, operating as intended, and producing the desired outcome.
- Formally notifies the DAA of the results of the certification process.
- Serves as primary liaison with the certification and accreditation coordinator, system points of contact, and the certification and accreditation team.
- Works with EIS to determine technical and non-technical points of contact for the system, to schedule a certification and accreditation kickoff meeting, and to coordinate the overall schedule for interviews, system testing, and delivery/review of documentation.

Federal Incident Manager

The Federal Incident Manager has the following responsibilities with respect to incident response:

- Coordinating and managing of all Federal and contractor resources.
- Overseeing and managing all plan development and after action activities related to the incident.
- Overseeing managing and team reviews.
- Reviewing and approving progress updates and report.

Incident Scribe

The Incident Scribe has the following responsibilities with respect to incident response:

- Documenting, consolidating, and managing all information pertaining to the incident.

Contract Incident Manager

The Contract Incident Manager has the following responsibilities with respect to incident response:

- Coordinating and managing of contractor resources.
- Working with the Communications Manager in the production and maintenance of the incident communications plan.
- Facilitating all plan development and after action activities related to the incident.
- Facilitating management and team reviews.
- Produces progress updates and report.

Communications Manager

The Communications Manager has the following responsibilities with respect to incident response:

- Producing, maintaining and executing the incident communications plan; and
- Coordinating, managing and communicating all communications from the OIT Incident response team to PBGC business units, management and staff, and vice versa.

Office of Inspector General

The Office of Inspector General has the following responsibilities with respect to incident response:

- Investigate complaints concerning suspected fraud or other violations of laws, mismanagement, gross waste of funds or resources, abuse of authority relating to PBGC's programs and operations, and dangers to public safety and health;
- Report to the Attorney General whenever there are reasonable grounds to believe that Federal criminal laws have been violated;
- Review existing or proposed legislation and regulations to make recommendations to PBGC and the Congress on the prevention and detection of fraud, waste, and abuse;
- Keep the agency head and the Congress fully informed about problems and deficiencies in programs administered by PBGC and the need for timely corrective action;
- Initiate investigations and to issue subpoenas to individuals or entities outside the Federal Government to obtain full access to documents and records.

9. **PROCEDURES**: OIT will be responsible for the policies and procedures established in the Information Assurance Handbook (IAH). Departments may request the creation, modification and deletion of Information Security policies using the procedures below.
 - a. The originator identifies the need for a new policy, or modification or deletion of an existing policy.

- i. For a new policy, the originator's office will develop a draft policy consistent with the format provided in this order.
 - ii. For a modification to an existing policy, the originator's office will develop a draft "revised" policy consistent with the format provided in this order.
 - iii. For the deleting of a policy, the originator's office will identify the policy to be deleted.
- b. The originator's office will prepare a paper which documents the request justification for the request.
- c. The originator's office will send the justification along with the rewrite of the policy to the Senior Agency Information Security Officer for review.
- d. The Senior Agency Information Security Officer will review the request and respond to the originator within ten (10) business days.
- e. OIT will update this Directive using the procedures outlined in Directive GA Part 05 Section: 01.

The reference provided below is a listing of all volumes in the IAH including the areas they pertain to. As changes are made to Federal statutes, regulations, and directives amendments to these volumes will become necessary and require republishing. OIT will update the IAH through PBGC's Directive System, GA 05-01.

Reference: (http://intranet/computer_support/security.cfm) provides access to:

- Volume 1, Access Control
- Volume 2, Awareness and Training
- Volume 3, Audit and Accountability
- Volume 4, Certification & Accreditation
- Volume 5, Configuration Management
- Volume 6, Contingency Planning
- Volume 7, Identification & Authentication
- Volume 8, Incident Response
- Volume 9, Maintenance
- Volume 10, Media Protection
- Volume 11, Physical & Environmental Protection
- Volume 12, Planning (PIA, SSP)
- Volume 13, Personnel Security
- Volume 14, Risk Assessment
- Volume 15, System & Services Acquisition
- Volume 16, System & Communications Protection
- Volume 17, System & Information Integrity
- Volume 18, Inventory Methodology
- Volume 19, Relevant Sources