**Pension Benefit Guaranty Corporation**

# Directive

**Subject: PBGC Privacy Program**

**Directive Number: IM 05-09**

**Effective Date:** **Originator: OGC**

Alice Maroni
Chief Management Officer

ALICE MARONI
Digitally signed by ALICE MARONI
Date: 2018.05.21 16:15:57 -04'00'

1. **PURPOSE**: This Directive establishes a framework to support a strong, multi-faceted PBGC privacy program in accordance with the Privacy Act, requirements issued by the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST).

2. **EFFECTIVE DATE**: This Directive replaces PBGC Order IM 05-09 dated October 13, 2010. This Directive is effective on the date shown above.

3. **SCOPE**: This Directive applies to all PBGC employees and contractors.

4. **AUTHORITIES & REFERENCES**:

   a. The Privacy Act of 1974, as amended
   b. The Freedom of Information Act of 1966, as amended
   c. The E-Government Act of 2002
   d. Internal Revenue Code § 6103
   e. OMB Circular A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act of 1974
   f. OMB Circular A-130, Management of Federal Information Resources
   g. OMB Memorandum M-03-18, Implementation of the E-Government Act of 2002
   h. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
   i. OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy
   j. OMB Memorandum M-06-16, Protection of Sensitive Agency Information

k. OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
l. NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
m. NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
n. NISTIR 8062, An Introduction to Privacy Engineering and Risk Management in Federal Systems
o. NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems
p. PBGC Directive IM 05-02, PBGC Information Security Policy
q. PBGC Directive IM 10-02, Safeguarding Tax Return Information
r. PBGC Directive IM 10-03, Protecting Sensitive Information
s. PBGC Directive IM 15-03, PBGC Records Management Program
t. PBGC Directive PM 10-05, Telework Program
u. PBGC Directive PM 30-01, Disciplinary and Adverse Actions
v. PBGC Directive FM 15-03, Suspension and Debarment

5. **BACKGROUND**: The PBGC requires that all employees and contractors (regardless of location) abide by the privacy policies set forth in this Directive to safeguard the Personally Identifiable Information (PII) collected, maintained, used, and disseminated by the PBGC. The Federal Government has enacted several laws, promulgated regulations, and issued guidance that establish federal and agency-level responsibilities for protecting PII, establish the duties of key privacy officials, set forth minimum privacy Controls (as defined below), and establish reporting requirements.

   This Directive, with the policies defined herein, recognizes the vast responsibility that PBGC employees and contractors have been entrusted with when working with PII and sets PBGC's policy for protecting PII, while balancing the need to perform PBGC's mission. This Directive also puts in place the guidelines that:

   a. Establishes the Risk Management Framework (RMF) aligned with NIST guidance.
   b. Protects PBGC's PII efficiently by providing flexibility in tailoring privacy Controls considering acceptable risks, mission needs, and operational factors, and collaborating with the Office of Information Technology (OIT) on security requirements.

6. **DEFINITIONS**:

   a. **Breach.** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) A person other than an authorized user accesses or potentially accesses PII or (2) An authorized user accesses or potentially accesses PII for an other than authorized purpose.
   b. **Control.** A safeguard or countermeasure prescribed for an Information System or an organization designed to safeguard its information and to meet a set of defined privacy 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's Information Systems.[1]

c. **Information System.** A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

d. **Personally Identifiable Information (PII).** Information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. PII includes information relating to individual participants and beneficiaries in covered pension plans, to PBGC employees, and to PBGC contractors.

e. **Record.** Any item, collection, or grouping of information, whether paper or electronic, about an individual that is maintained in a PBGC System of Records including, but not limited to his/her education, financial transactions, medical history, and criminal or employment history, and that contains his/her name, or identifying number (such as a social security number), symbol, or other identifying particular assigned to the individual such as a finger or voice print or a photograph.[2]

f. **System of Records.** A group of any Records under the control of the PBGC from which information is retrieved by the name or by some identifying number, symbol, or other identifying particular assigned to an individual.

g. **System of Records Notice (SORN).** A notice published in the Federal Register that describes a PBGC System of Records.

7. **POLICY:** It is PBGC Policy to protect the PII entrusted to it commensurate with the sensitivity, criticality, and value of the information. PBGC shall:

a. Implement a privacy risk management process to protect PII held by PBGC or on behalf of PBGC.

b. Comply with OMB and NIST guidance with respect to privacy.

c. Work with the PBGC business units and IT to categorize all PBGC Information Systems that process, store, or transmit PII including externally owned or hosted systems in accordance with Federal Information Processing Standard (FIPS) 199, implement the appropriate privacy Controls from the current version of NIST SP 800-53, and assess the implementation of the privacy Controls.

d. Address risk management as early as possible in the acquisition or modification of an IT or third-party system.

e. Leverage the agency's assessment and authorization system to manage system authorizations and the implementation of privacy Controls.

f. Collaborate with OIT to establish a process to deploy privacy and security Controls throughout PBGC and third-party systems consistent with NIST guidance, the FIPS, and other applicable federal mandates.

[1] *See* NIST SP 800-53, rev. 4, at 2.

[2] 5 U.S.C. § 552a(a)(4). Note that the definition of "record" varies between statutory frameworks. Other directives may use different definitions.

g. Ensure appropriate use of PII to fulfill PBGC's missions and functions, to limit the use of PII to the minimum necessary, and to eliminate the use of PII in non-production environments.
h. Establish a process for responding, within thirty (30) days, to complaints, concerns, or questions from individuals about the organizational privacy practices.
i. Comply with the procedures, processes, and guidance developed and disseminated by the Privacy Office via the Privacy Office Intranet page, email, or any other methods to address privacy compliance, responsibilities, management commitment, incident response, and coordination among organizational entities. Standards, procedures, processes, and guidance derived from this Directive are incorporated into this policy.
j. Disseminate guidance to implement this Directive and NIST privacy Controls.

8. **POLICY DEVIATIONS**:

a. The Senior Agency Official for Privacy (SAOP) has the authority to approve a privacy policy deviation. Requests for a deviation from a privacy policy must come from a Department Director or higher and adhere to the Privacy Policy Deviation Process.
b. Documentation of the request and adjudication of the request shall be maintained by the Privacy Office.
c. Approved policy deviations shall be reviewed annually.
d. Any change in the underlying privacy risks that led to the approved policy deviation should be reported to the Privacy Office as soon as practicable for a determination on whether the approved deviation is still valid and necessary.

9. **NON-COMPLIANCE**:

a. Individuals who do not comply with this policy, including the standards, procedures, processes, and guidance developed and disseminated by the Privacy Office, may be subject to corrective, disciplinary and/or adverse action, as described in:

(1) PBGC Directive PM 30-1, for employees.
(2) PBGC Directive FM 15-3, for contractors.

b. Individuals may also be denied access to PBGC Information Systems that contain PII.
c. An Information System that does not comply with this policy, including the procedures, processes, and guidance developed and disseminated by the Privacy Office, will be subject to SAOP review which may result in the SAOP recommending that the system be barred from operating until the system is brought into compliance or an exemption from the privacy policy is granted by the SAOP.
d. The Privacy Act of 1974 contains criminal provisions for mishandling PII, operating a System of Records without meeting the notice requirements, and for obtaining records under false pretenses. *See* 5 U.S.C. § 552a(i)(1)-(3).

10. **PROCEDURES**: Documents implementing privacy Controls and this policy will be posted to the Privacy Intranet page. Published documents will be reviewed annually. Unless otherwise noted, the Privacy Office will offer training to stakeholders on new and revised procedures, processes, and guidance.

11. **RESPONSIBILITIES**:

a. **PBGC Director.**

(1) Retains overall responsibility and accountability for privacy protections commensurate with the risk and harm to PBGC's operations, assets, and the individuals it serves.
(2) Ensures that privacy policies are developed and implemented to mitigate the risk to PBGC's operations, assets, and the individuals it serves.

b. **Senior Agency Official for Privacy (SAOP).** The SAOP is primarily responsible for the Corporation's privacy policy and exercises a central role in overseeing, coordinating, and facilitating the organization's privacy compliance efforts. This role includes:

(1) Providing guidance to the PBGC Director and senior leadership to ensure that PII is protected in a manner in compliance with the Privacy Act, the E-Government Act, and OMB and NIST guidance.
(2) Designating a Chief Privacy Officer (CPO).
(3) Reviewing the organization's privacy procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and Federal guidance.
(4) Where additional or revised procedures are identified, consulting and collaborating with the appropriate PBGC offices in developing, adopting, and implementing these procedures.
(5) Ensuring PBGC employees and contractors receive appropriate training and education regarding their privacy protection responsibilities.
(6) Playing a central policy-making role in the organization's development and evaluation of legislative, regulatory, and related policy proposals implicating privacy issues.
(7) Determining whether the Breach Response Team (BRT) should be convened.
(8) Chairing the BRT for privacy incidents not involving Information Systems and co-chairing the BRT with the Chief Information Security Officer (CISO) for privacy incidents involving Information Systems.
(9) Reviewing and adjudicating deviations from privacy policies.
(10) Preparing and submitting various privacy-related reports such as the annual Senior Agency Official Privacy Report to OMB required by the Federal Information Security Management Act ( FISMA).
(11) Working closely with the CISO and OIT which have Information System

security responsibilities.

c. **Chief Information Officer (CIO).** The CIO is primarily responsible for ensuring that an agency-wide information security program is developed and maintained.

(1) Collaborating with the SAOP to implement the Privacy Office's and the Enterprise Cybersecurity Division's (ECD) incident response plans in the event of a Breach involving an Information System.
(2) Working closely with the CPO and SAOP to safeguard PII maintained or transmitted by an Information System.

d. **Chief Privacy Officer (CPO).** The CPO is responsible for:

(1) Developing, documenting, and implementing an agency-wide privacy program to protect the PII that the agency collects, maintains, uses, and disseminates to execute, and in support of, the mission of PBGC.
(2) Developing and maintaining privacy policies, procedures, processes, training, and Controls to address all privacy requirements set forth in federal law, regulations, and guidance.
(3) Collaborating with ECD to offer privacy common Controls.
(4) Assisting stakeholders to implement system Controls.
(5) Ensuring that Breaches are reported and that individuals impacted entities are notified of Breaches when deemed appropriate.

e. **Chief Information Security Officer (CISO).** The CISO develops, documents, and implements an agency-wide IT-security program including system and security Controls related to the protection of PII for the information and Information Systems that support the operations and assets of the agency.

(1) Collaborating with the SAOP to implement the Privacy Office's and the ECD's incident response plans in the event of a Breach involving an Information System.
(2) Working closely with the CPO and SAOP to safeguard PII maintained or transmitted by an Information System.

f. **Information System Security Managers (ISSM).**

(1) Ensures that the operational security and privacy posture is managed for Information Systems and programs under their control.
(2) Participates as member of PBGC Cybersecurity and Privacy Council.
(3) Ensures that the monitoring, testing, and evaluation of the effectiveness of privacy policy, procedures, practices, and privacy Controls are performed and completed with a frequency depending on risk as recommended by the Privacy Office.
(4) Ensures that solicitation requirements for IT hardware, software, and professional services have the appropriate references and clauses needed to

address privacy in the final solicitation package.

g. **Information System Security Officers (ISSO).**

(1) Communicates directives, policy, and guidance to their business unit and relays issues to the appropriate parties.
(2) Ensures work products and documents are properly labeled and maintained according to privacy requirements.
(3) Ensures agency privacy policies, procedures, and Control techniques are implemented to protect sensitive information within their assigned business area.

h. **Information Owners/Information System Owners (IO/ISO).**[3]

(1) Collaborates with the Contracting Officer Representative on 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 privacy requirements.
(3) Ensures the Information System is operated according to the agreed upon privacy requirements.
(4) Manages the system privacy Controls and associated organizationally defined parameters.
(5) Ensures that adequate measures and procedures are implemented to protect the data residing on their system(s).
(6) Safeguards the information he/she owns and retains that responsibility when information is shared with or provided to other organizations.

i. **Breach Response Team (BRT).** The BRT is a multi-disciplinary core team with expertise necessary to respond to a Breach. The BRT will implement the Privacy Office Breach Response Plan.

j. **Office of the Inspector General (OIG).** The Inspector General supports PBGC's Privacy Program and will conduct the recommended actions to the extent it does not infringe on OIG's independence.

(1) In the event of a loss or compromise of PII involving a suspected violation of law, rule, or regulation, the OIG will be notified by the BRT so that the OIG can take appropriate action.

k. **Office of Policy and External Affairs (OPEA).** In the event of a major loss or

[3] Information System Owners oversee internal Information Systems; Information Owners oversee systems hosted remotely by another federal agency, a commercial entity, or the cloud.

compromise of PII, the SAOP and CPO will coordinate with OPEA to:

(1) Respond to media inquiries.
(2) Communicate with Congress, as necessary.
(3) Coordinate public outreach.

l. **Procurement Department (PD).** The Procurement Department is responsible for:

(1) Ensuring appropriate clauses concerning protection of PII are included in PBGC solicitations and contracts.
(2) Ensuring clauses that require contractors to comply with this directive, PBGC IM-10-3, Protecting Sensitive Information, and other PBGC privacy policies and procedures are included in PBGC solicitations and contracts.
(3) Providing contract management and oversight of contractor compliance with PBGC privacy policies and procedures.

m. **Records Officer.** The Records Officer is responsible for developing integrated records management policies that take privacy considerations into account. The Records Officer also supports the privacy program by:

(1) Participating in privacy awareness and outreach efforts.
(2) Assisting in the development of training materials.

n. **Department Directors/Managers.** All PBGC Department Directors and Managers are responsible for promoting the PBGC privacy program within their departments and divisions by:

(1) Supporting Privacy Program outreach efforts.
(2) Ensuring employees complete privacy training.
(3) Ensuring privacy incidents are reported.
(4) Implementing courses of action recommended by the CPO and/or BRT in response to Breaches.

o. **PBGC Employees and Contractors.** Protecting PII is the responsibility of every PBGC employee and contractor. Additionally, all employees and contractors are responsible for:

(1) Understanding their obligations with respect to PII.
(2) Following PBGC privacy procedures when handling PII whether in electronic or paper format (*See* PBGC Directive IM 10-03, Protecting Sensitive Information).
(3) Assisting in reporting, assessing, training, and improving the way the Corporation handles PII.

p. **Privacy Specialists.** Privacy Specialists are responsible for supporting the SAOP and CPO in coordinating and implementing PBGC's privacy compliance efforts.

This role includes:

(1) Developing and implementing privacy policies, procedures, processes, and training to address privacy requirements set forth in federal laws, regulations, and guidance.
(2) Working with stakeholders to assess and implement privacy Controls.
(3) Ensuring that Breaches are reported and that individuals and impacted entities are notified of Breaches when deemed appropriate.