Pension Benefit Guaranty Corporation

Order

Subject: Privacy Program

Directive Number: IM 05-9

Effective Date: 10/13/10 **Originator: OGC**

Vincent K. Snowbarger
Acting Chief Management Officer

---

1. **PURPOSE**: This Order establishes a framework to support a strong, multi-faceted PBGC privacy program, and to instill and support a culture of privacy protection throughout the Corporation.

2. **SCOPE**: This Order applies to all PBGC employees and contractors.

3. **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. PBGC Order IM 10-3, Protecting Sensitive Information
   f. PBGC Order IM 10-2, Safeguarding Tax Return Information
   g. PBGC Order PM 30-1, Disciplinary and Adverse Actions
   h. OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records about Individuals
   i. OMB Memorandum M-03-18, Implementation of the E-Government Act of 2002 (Aug. 1, 2003)
   j. OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 26, 2003)

k. OMB Memorandum M-05-08, Designation of Senior Agency Officials for Privacy (Feb. 11, 2005)
l. OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
m. OMB Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006)
n. OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments (July 12, 2006)
o. OMB Memorandum, Recommendations for Identity Theft Related Data Breach Notification (Sept. 20, 2006)
p. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
q. NIST Special Publication 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
r. Executive Order 13392, Improving Agency Disclosure of Information

4. **BACKGROUND**: This Order establishes a formal, comprehensive strategic framework that integrates PBGC's Privacy Program standards, policies, procedures, training and outreach requirements, as well as roles and responsibilities. The framework supports PBGC management efforts in addressing privacy risks and promotes best practices in privacy across the Corporation.

5. **DEFINITIONS**:

a. **Breach.** A loss of control; compromise; unauthorized disclosure, acquisition, or access; or any similar term referring to situations involving an other than authorized purpose where persons other than authorized users have access or potential access to PII, whether physical or electronic.

b. **Computer Based Training (CBT).** Training courses using the computer as the primary delivery method of instruction.

c. **Individual.** A living person who is either a U.S. citizen or an alien lawfully admitted for permanent residence.

d. **Information System.** Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, creation, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Examples include desktop and laptop computers assigned to staff.

e. **System Owner.** The PBGC official identified in the system of record notice (SORN) who is responsible for the operation and management of the System of Records (SOR), or the PBGC official who is designated to conduct a privacy impact assessment for an Information System.

f. **Personally Identifiable Information (PII).** Any information about an Individual that is subject to the Privacy Act of 1974, 5 U.S.C. § 552a, such as information relating to individual participants and beneficiaries in covered pension plans, or individual PBGC employees or contractors. PII also includes nonpublic information about an individual that, when combined with the individual's name, can be used to distinguish or trace an individual's identity, such as the individual's social security number, date or place of birth, and mother's maiden name.

g. **Privacy Impact Assessment (PIA).** The multi-disciplinary process, required under section 208 of the E-Government Act of 2002, by which PBGC analyzes and mitigates the privacy risks associated with the development or procurement of any new information system that contains PII, the alteration of any such existing system, or any new electronic collection of information from ten or more persons.

h. **Program Office (PO).** Any office within PBGC that operates a Privacy Act SOR, collects information from ten or more entities or members of the public, and/or has responsibility for an information system that contains PII.

i. **Record.** Any item, collection, or grouping of information, whether paper or electronic, about an Individual that is maintained in a PBGC SOR, 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.

j. **System of Records (SOR).** 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.

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

l. **United States Computer Emergency Response Team (US-CERT).** The Federal security incident-handling center located within the Department of Homeland Security.

6. **POLICY**: Privacy stewardship and governance are critical to a successful privacy program and can reduce the risk that government programs erode privacy protections and ultimately lose the public's trust. Protecting PII is an integral part of PBGC's business operations and must be a core consideration for every PBGC department, employee, and contractor. All PBGC PII must be reasonably protected regardless of the medium on which it is stored, the information systems that process, store, or transmit the information, or the methods by which the information is moved.

7. **RESPONSIBILITIES**:

a. **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) reviewing the organization's privacy procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and Federal guidance;
(2) where additional or revised procedures are identified, consulting and collaborating with the appropriate PBGC offices in developing, adopting, and implementing these procedures;
(3) ensuring PBGC employees and contractors receive appropriate training and education regarding their privacy protection responsibilities;
(4) as the Chair of the Privacy Steering Committee, playing a central policy-making role in the organization's development and evaluation of legislative, regulatory, and related policy proposals implicating privacy issues;
(5) preparing and submitting various privacy-related reports, such as the annual Senior Agency Official Privacy Report to OMB required by FISMA.
(6) Because privacy and security are inter-related, the SAOP works closely with the CIO and OIT, which has information system security responsibilities.

b. **Chief Information Officer (CIO).** With respect to privacy, the CIO is primarily responsible for developing and maintaining the agency-wide information security program, including system and security controls related to the protection of PII, and ensuring all systems comply with the security program.

(1) In the event of a loss or compromise of PII, the CIO is responsible for collaborating with the SAOP and assisting the BRT in the development and execution of a corporate response plan.
(2) Because privacy and security are inter-related, the CIO works closely with the Office of the General Counsel (OGC), which has Privacy Act and Freedom of Information Act responsibilities.

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

(1) assisting in development of PBGC's privacy and data protection procedures and policies;
(2) developing privacy training materials;
(3) educating PBGC employees and contractors about protecting PII through outreach and training initiatives;

(4) developing and providing guidance to information system owners on conducting PIAs and drafting SORNs; and
(5) coordinating the review and completion of PIAs and SORNs for PBGC information systems.
(6) responsible for notifying impacted entities of breaches, when deemed appropriate.

d. **Senior Agency Information Security Officer (SAISO).** The SAISO serves as the CIO's primary liaison to the agency's information system owners with respect to IT security issues and concerns, including those involving PII.

(1) Because privacy and security are inter-related, the SAISO works closely with the Office of the General Counsel (OGC) and collaborates with the SAOP on privacy polices.
(2) As co-chair of the BRT, the SAISO works with the SAOP to lead the BRT in addressing incidents involving the possible compromise or loss of PII and developing corporate response plans as appropriate.
(3) The SAISO is also responsible for reporting breaches and potential breaches of PII to the United States Computer Emergency Response Team (US-CERT).

e. **Privacy Steering Committee.** The Privacy Steering Committee is chaired by the SAOP. Its members are identified in section 8(d) below. The duties and responsibilities of the Privacy Steering Committee include:

(1) monitoring security and privacy guidance issued by the Office of Management and Budget (OMB), the Department of Homeland Security, and other sources to assist PBGC in developing new or revising existing policies and procedures to comply with the new guidance;
(2) reviewing the effectiveness of existing PBGC privacy policies, procedures, and technologies/tools, and recommending any needed changes;
(3) making recommendations on implementing privacy-related security controls as part of PBGC's agency-wide information system security plan;
(4) making recommendations on developing and delivering training programs for PBGC employees and contractors on protecting sensitive information;
(5) making recommendations on conducting PIAs for new or modified information systems;
(6) following up on recommendations to ensure that they are implemented effectively.

f. **Breach Response Team (BRT).** The BRT is a multi-disciplinary core team with expertise necessary to respond to a data breach. The BRT is co-chaired by the Senior Agency Official for Privacy (SAOP) (see section 7.a) and the Senior Agency Information Security Officer (SAISO) (see section 7.d) and is responsible for:

(1) developing, updating and maintaining corporate breach response procedures;
(2) in the event of a breach, assessing the likely risk of harm and the level of risk; identifying any additional resources required to properly respond to the breach; and recommending an appropriate corporate response plan.

g. **Office of the General Counsel (OGC).** OGC works closely with the CIO, information system owners, the Office of Information Technology (OIT), and the Records Management Officer to administer the Privacy Program and coordinate privacy initiatives. OGC has responsibility for:

(1) reviewing completed PIAs and SORNs;
(2) providing legal advice related to the Privacy Act and the Freedom of Information Act;
(3) coordinating with the BRT to ensure the corporate response plan for a breach involving PII is successfully executed in compliance with Federal laws and regulations.

h. **Office of the Inspector General (OIG).** In the event of a loss or compromise of PII involving a suspected violation of criminal law, the OIG will be notified by the BRT so that the OIG can take appropriate action.

i. **Privacy Liaisons.** Privacy liaisons are Federal employees designated by a PBGC Department Director who are responsible for assisting the CPO by:

(1) identifying the need for new and revised PIAs and SORNs within their respective departments;
(2) preparing input for reports required under the Privacy Act;
(3) serving as a first point-of-contact to staff within their departments on privacy issues;
(4) assisting with routine privacy matters; and
(5) referring more complex matters to OGC's privacy staff.

m. **Communications and Public Affairs Department (CPAD).** In the event of a loss or compromise of PII, CPAD is responsible for:

(1) responding to media inquiries;
(2) coordinating with OGC's Disclosure Division in responding to FOIA inquiries; and
(3) if necessary, initiating press releases.

n. **Legislative and Regulatory Department (LRD).** As appropriate, LRD serves as the Corporation's liaison with committees and Members of the Congress with respect to incidents involving a loss or compromise of PII. LRD is also responsible for publishing new and altered SORNs in the Federal Register.

o. **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;

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

(1) participating in privacy awareness and outreach efforts; and
(2) assisting in the development of training materials.

k. **Department Directors.** All PBGC Department Directors are responsible for promoting the PBGC privacy program within their departments by:

(1) supporting Privacy Program outreach efforts;
(2) ensuring employees – including designated privacy liaisons (see sections 7.i and 8.c) – attend appropriate privacy training;
(3) ensuring privacy incidents are reported;
(4) cooperating with and responding to requests for information from the Privacy Steering Committee; and
(5) implementing courses of action recommended by the Breach Response Team (BRT) (see sections 7.f and 8.f) in response to breaches involving PII.

(i) The Office of the Inspector General supports PBGC's Privacy Program and will conduct the activities established in section 7.k to the extent it does not infringe on its independence.

l. **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-10-3, Protecting Sensitive Information), and

(3) assisting in reporting, assessing, training, and improving the way the Corporation handles PII.

8. **PROCEDURES**:

a. Training.

(1) All PBGC employees and contractor personnel shall complete privacy training, computer-based or in-person, annually. New PBGC employees and contractor personnel shall complete training before gaining access to the PBGC network and/or electronic PII. The training shall include an overview of Federal and agency-specific privacy requirements, policies, and procedures.

(2) Privacy liaisons and PBGC employees and contractor personnel whose primary duties include handling PII, or who handle large amounts of PII, shall also receive additional, targeted training, as determined by the SAOP.

b. Outreach.

(1) PBGC is committed to creating a culture of privacy, in which all employees and contractors are aware and considerate of privacy principles, information and responsibilities. A strong awareness and communications effort is key to creating this environment. The CPO shall coordinate an ongoing, multi-disciplinary privacy awareness and communications effort that consists of several components, *e.g.*:

(a) Global messages and tips focused on privacy issues;
(c) Privacy policies and procedures;
(d) Privacy events.

(2) All PBGC Directors, managers, and supervisors shall support Privacy Program outreach efforts, and encourage the participation of PBGC components and employees in such efforts.

c. Privacy Liaisons.

(1) Each PBGC Department Director shall designate a privacy liaison to:

(a) Serve as the first point of contact for PBGC employees and contractors on routine privacy matters that arise within the Department.
(b) Refer more complex privacy matters to OGC's privacy staff.
(c) Assist in identifying the need for new and revised PIAs and SORNs.

(2) The CPO, or his or her designee, shall ensure the liaison receives in-person training to adequately prepare the liaison to perform these duties.

(4) A list of departmental liaisons will be posted on PBGC's Privacy Intranet webpage.

d. Privacy Steering Committee.

(1) Purpose.

(a) The Privacy Steering Committee serves as an interdepartmental coordinating committee to review and make recommendations on policies and procedures established to protect PII and other sensitive information in any format. In particular, the Privacy Steering Committee shall recommend or take actions that maximize safeguards for preventing the intentional or negligent misuse of PII.

(2) Membership.

(a) SAOP serving as a co-chair
(b) SAISO serving as a co-chair
(b) CPO
(c) Chief Operating Officer
(d) CIO (optionally)
(e) Chief Insurance Program Officer (or designee)
(f) Chief Financial Officer (or designees)
(h) A representative from the Office of Policy and External Affairs
(i) A representative from the Benefits Administration and Payments Department
(j) A representative from the Human Resources Department
(k) A representative from the Facilities and Services Department
(l) Records Management Officer

(3) Meetings. The Privacy Steering Committee will meet at least monthly and minutes of meetings will be kept and distributed to Committee members.

(4) Working Groups. Working groups of the Privacy Steering Committee members and designated members from PBGC components may be established to study and make recommendations on relevant issues or to carry out specific activities relevant to the Privacy Steering Committee's purpose. Working group leaders will be appointed by the Committee Chair.

e. Information Collection Procedures

(1) Privacy Impact Assessments (PIAs).

(a) Before developing any new information system that contains PII, altering any such existing system, or commencing any new electronic collection of information from ten or more members of the public, the PBGC program office (PO) for the system will ensure a PIA is accomplished. The PO will appoint a system owner to conduct the PIA.

(i) The system owner will consult with the CPO for initial guidance during the conceptual planning phase of the system development life cycle.

(ii) The system owner will provide such information as is necessary to assist the CPO in determining if a PIA is required. If the PII status of a system is in dispute, the CPO will work with the system owner and the SAISO to resolve the dispute. If the dispute cannot be resolved, the SAOP determines whether a PIA is required.

(iii) The system owner will organize a PIA planning session that will include representatives from OGC and OIT to provide PIA training and assist in charting out an appropriate course of action.

(iv) The system owner will conduct the PIA in accordance with guidance developed by OMB and the CPO. The system owner will consult with the multi-disciplinary team as necessary to identify and mitigate risks to personal privacy.

(v) The system owner will analyze from a risk perspective all identified privacy risks and appropriately address them.

(vi) The system owner will follow the procedures outlined in section 8.f below, if the PIA identifies the need for a Privacy Act SORN and/or a collection of information from ten or more members of the public.

(vii) The system owner will route the draft PIA for clearance by the SAOP and the SAISO.

(viii) The CPO ensures PIA summaries approved for public release are submitted to OMB, as necessary, and posted on the PBGC Privacy web site.

(ix) The system owner, CPO, and SAISO will maintain a copy of final approved PIAs. The CPO will maintain the official copies.

(x) A PIA is a living document that must be updated when a major change in the system occurs. Examples of system changes that may require completing a new PIA are listed in OMB M-03-22 (reference 3.e) (*e.g.*, new uses of existing IT systems; merging of government databases; user-authentication technology is newly applied to systems accessed by the public).

(xi) System owners are responsible for determining when reviews and updates are required. The PO will periodically review PIAs to ensure they comply with current system practices.

(xii) On at least an annual basis, the CPO will contact all system owners and remind them of the requirement to review PIAs and make necessary updates. The system owner must certify that he or she has reviewed the PIA and determined no changes are necessary, or identify and submit proposed changes to the CPO.

NOTE**:** Once a system expires or is retired and no longer in operation, the system's PIA should be retired.

(2) System of Records Notices (SORNs).

(a) PBGC provides notification to individuals who are asked to supply PII, informing them of the authority for collection, the principal purpose for which the information is collected, the routine uses of the information, and any consequences of not providing the information. Methods of notification include, but are not limited to, Privacy Act SORNs and web site policy statements.

(b) Before operating, altering, or deleting an agency SOR and before claiming any exemptions to such a system, PBGC will provide proper notice in the Federal Register. **Operating an unpublished system of records is a criminal violation.**

(i) The PO will consult with the CPO for initial guidance.

(ii) The PO will appoint a system owner for the SOR.

(iii) The system owner will draft the notice creating or altering the system of records with the CPO's assistance.

(iv) The system owner will submit the draft SORN to OGC for review and coordination with LRD.

(v) LRD will submit the draft SORN to the Federal Register for public comment.

(vi) The SAOP will submit any report to the House of Representatives, the United States Senate, and OMB required by OMB Circular A-130 (reference 3.c).

(vii) The system owner must wait 40 days for public comments. If substantive comments are submitted at any time within the 40 day period, the system owner must address the comments, amend the draft SORN, and re-submit the amended SORN for coordination and publication in the Federal Register. When the draft SORN is re-submitted to the Federal Register, the 40-day waiting period for public comment begins again.

(viii) If no substantive comments are received within the 40 day public comment period, the SAOP publishes the final SORN on PBGC's public web site.

(ix) The SORN process is complete, pending other requirements related to putting the SOR into production (e.g., security certification and accreditation). If all other requirements are met, the SOR may proceed to production.

(x) System owners must biennially review SORNs to ensure they accurately describe the systems of records, and notify OGC of any required changes.

(xi) Changes or amendments to SORNs are published in the Federal Register according to the procedures in this section.

f. Breach Response Team

(1) Purpose.

(a) The Breach Response Team (BRT) serves as an interdepartmental response team that is tasked with coordinating the corporate response to a breach involving PII. This involves assessing the likely risk of harm resulting from the breach, determining the level of risk, and

determining whether additional steps are required in accordance with the breach response procedures developed by the BRT. These additional steps may include, but are not limited to, notifying the affected parties, OIG, involving law enforcement, providing credit monitoring services, and other steps that should be taken to avoid a recurrence.

(2) Members.

(a) The core members of the BRT include:

(i) SAOP (co-chair)
(ii) SAISO (co-chair)
(i) CPO
(ii) CIO (optionally)
(iii) A representative from CPAD
(iv) A representative from LRD

(b) In the event of a breach, the Director of the PBGC Department in which the breach occurred, or his designee, shall assist the BRT as an ad hoc member.

(c) In addition, the BRT co-chairs may designate other ad hoc members, as necessary. For instance, in the event that criminal activity is suspected, OIG would be designated as an ad hoc member.

g. Incident Reporting

(1) A breach or suspected breach of PII can include any of the following:

(a) possible or actual unauthorized disclosure or acquisition of PII;
(b) possible or actual loss or theft of physical documents or electronic PII; and
(c) possible or actual loss or theft of electronic equipment containing PII.

(2) When an Incident is Discovered or Suspected.

(a) When an employee or contractor discovers or suspects that a breach of PII has occurred, he will immediately send a report of the incident to PRIVACY_BREACH@pbgc.gov with a copy to his supervisor or, if he is a contractor, COTR.

(b) The email should include the following information:

(i) date and time of the breach;
(ii) location of the breach;
(iii) the nature of the breach (e.g., a misdirected document or email, the loss of computer hardware);
(iv) the type of PII involved (e.g., name, social security number, date of birth, address);
(v) people involved;
(vi) any immediate harm known or observed;
(vii) any corrective action already taken.

(c) Report to US-CERT.

(i) The SAISO is responsible for reporting breaches to US-CERT. OGC will provide, as needed, assistance to the SAISO to ensure timely reporting to US-CERT.

[NOTE: During a transition period, OGC will have responsibility for reporting breaches to US-CERT. The SAISO and the SAOP will advise users when the transition period has ended. No revision to this Directive will be issued at that time.]

(ii) Within one hour of receipt of an incident report to PRIVACY_BREACH@pbgc.gov or by other means, PBGC must submit a report to US-CERT describing the incident. This reporting requirement does not distinguish between potential and confirmed breaches.