Pension Benefit
Guaranty Corporation

Directive

Subject: Protecting Sensitive Information

Directive Number: IM 10-03

Effective Date: 10/30/2015 **Originator: OGC**

Alice C. Maroni
Acting Director

1. **PURPOSE:** This Directive establishes the policies and procedures for protecting sensitive information, including personally identifiable information (PII).

2. **EFFECTIVE DATE:** This Directive replaces and supersedes the Pension Benefit Guaranty Corporation's (PBGC) Directive IM 10-3 dated 4/23/08 and is effective on the date shown above.

3. **SCOPE:** This Directive applies to all PBGC employees and contractors and to all PBGC systems that stores, processes, or transmits sensitive information.

4. **AUTHORITIES:**

   a. Freedom of Information Act, 5 U.S.C. § 552.
   b. Privacy Act of 1974, 5 U.S.C. § 552a.
   c. Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
   d. Trade Secrets Act, 18 U.S.C. § 1905.
   e. Internal Revenue Code, I.R.C. § 6103, *Confidentiality and Disclosure of Returns and Return Information*.
   f. Internal Revenue Code, I.R.C. § 7213, *Unauthorized Disclosure of Information*.
   g. Clinger-Cohen Act, 40 U.S.C. 1401 *et seq.*
   h. Procurement Integrity Act, 41 U.S.C. §§ 2101-2107.
   i. Paperwork Reduction Act, 44 U.S.C. §§ 3501-3520.
   j. E-Government Act of 2002, 44 U.S.C. Ch. 35 *et seq.*
   k. Federal Information Security Management Act of 2002, 44 U.S.C. § 3501 *et seq.*
   l. Management and Promotion of Electronic Government Services, 44 U.S.C. §§ 3601-3606.
   m. Exec. Order 13,556, 75 Fed. Reg. 68,675, *Controlled Unclassified Information* (Nov. 4, 2010).
   n. Federal Acquisition Regulations, 41 C.F.R. § 3.104.
   o. Federal Information Processing Standard Publication 140-2.

p. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 12, 2004).
q. Office of Management and Business (OMB) Circular A-130, *Management of Federal Information Resources* (rev. Nov. 28, 2000).
r. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 30, 2003).
s. OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy* (Feb. 11, 2005).
t. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information* (June 23, 2006).
u. 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).
v. OMB Memorandum M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials* (Jan. 11, 2007).
w. OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007).
x. OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems* (Nov. 18, 2013).
y. OMB Memorandum M-15-01, *Guidance on Improving Federal Information Security and Privacy Management Practices* (Oct. 3, 2014).
z. PBGC Directive FM 15-03, *Suspension and Debarment Program.*
aa. PBGC Directive IM 05-02, *PBGC Information Security Policy.*
bb. PBGC Directive IM 05-04, *Use of Information Technology Resources.*
cc. PBGC Directive IM 05-09, *Information Privacy Program.*
dd. PBGC Directive IM 10-02, *Safeguarding Tax Return Information.*
ee. PBGC Directive IM 10-05, *Media Relations.*
ff. PBGC Directive PM 30-01, *Disciplinary and Adverse Actions.*
gg. PBGC Office of Information Technology Glossary of Terms.
hh. PBGC Records Management Program Interim Guidance.

5. BACKGROUND: This Directive provides guidance to PBGC departments, employees, and contractors[1] about PBGC's policies and procedures promulgated to establish and strengthen protections for sensitive information held by PBGC.

6. DEFINITIONS:

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

[1] Hereinafter, the term "contractor" may refer to both an entity that contracts with PBGC, and an individual who is employed by a contractor who performs contracted for services for PBGC, but is not an employee of PBGC.

b. **Contracting Officer's Representative (COR)**. The official designated to provide technical direction to contractors and to monitor the progress of the contractor's work.

c. **Controlled Unclassified Information (CUI)**. Information that requires safeguarding and/or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding classified information.

d. **Data extract**. Any sensitive information downloaded or copied from a PBGC database.

e. **Data masking**. The process of obscuring specific data elements to replace sensitive data with realistic—but not real—data. This ensures that otherwise sensitive information is not exposed to unauthorized individuals or inappropriate uses in non-production environments.

f. **Information owner**. The PBGC official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

g. **Information security**. The process of protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
   (1) *integrity*, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
   (2) *confidentiality*, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
   (3) *availability*, which means ensuring timely and reliable access to and use of information.

h. **Information system**. A discrete set of resources organized to collect, process, maintain, use, share, disseminate, or dispose of information.

i. **Information system owner**. The PBGC official responsible for the overall procurement, development, integration, modification, security and operation and maintenance of an information system.

j. **Need-to-know exception**. The Privacy Act exception that allows disclosure of Privacy Act protected information "[t]hose officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."

k. **Network**. Two or more PBGC information systems that are linked to share resources, exchange files, or allow electronic communications.

l. **Personally identifiable information (PII)**. Any information about an identifiable individual, maintained by PBGC including, but not limited to, information about an individual's employment, financial history, medical

history, education, family, and other information that can be used to distinguish or trace an individual's identity, such as an individual's name, social security number, date and place of birth, mother's maiden name, and biometric records.

m. **Privacy Breach**. *See* "Breach."

n. **Privacy Impact Assessment (PIA)**. An analysis of how information is/will be handled: (i) to ensure 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 an 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.

o. **Privacy Threshold Assessment (PTA)**. An analysis of how information is/will be handled that results in the determination of whether a PIA is necessary.

p. **Security Incident**. A computer-based or network-based activity which results (or may result) in misuse, damage, denial of service — including viruses, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

q. **Sensitive Information**. Information that has a degree of confidentiality such that loss, misuse, unauthorized access, or modification of it could compromise the element of confidentiality and thereby adversely affect PBGC's business operations, plans or participants of pension plans insured or trusteed by PBGC, or the privacy of individuals covered under the Privacy Act. Sensitive information includes, but is not limited to, agency records in electronic or hard copy format that contain:
   (1) PII (see (l) above)
   (2) Confidential business information submitted to PBGC by a plan sponsor or controlled group member, or information required to be submitted under ERISA
   (3) Confidential cost or proprietary information submitted in response to a PBGC request for proposals (RFP), or PBGC source selection information protected from disclosure under the Procurement Integrity Act
   (4) Tax returns, taxpayer identification numbers, and tax return information obtained from the Internal Revenue Service or directly from a private person or entity
   (5) Strategic documents such as position/decision papers or other items that could harm PBGC if inappropriately disclosed
   (6) Sensitive or proprietary information received from vendors and plan sponsors
   (7) Exploitable network information such as network diagrams, IP addresses, or firewall rule sets

(8) Exploitable IT system information such as computer program source code or logic, vulnerability scan results, patch levels, users' passwords

(9) Inter-agency or intra-agency memoranda or letters reflecting pre-decisional deliberations, internal personnel rules and practices, and other internal documents

(10) Information concerning EEO complaints, counseling, hearings, or investigations

(11) Any other nonpublic information that an employee or contractor knows, or reasonably should know, is considered confidential by PBGC or by the person or entity that submitted the information to PBGC

7. POLICY: It is PBGC's policy to protect the confidentiality, integrity, and availability of sensitive information from unauthorized disclosure and access by properly safeguarding, disseminating, destroying such information in accordance with applicable laws and regulations. All PBGC employees and contractors are responsible for protecting sensitive information.

8. RESPONSIBILITIES:

a. **PBGC Director.**

(1) Bears overall responsibility for protecting sensitive information.

(2) Appoints a Chief Information Officer (CIO).

(3) Appoints a Senior Agency Official for Privacy (SAOP).

b. **Chief Information Officer (CIO).**

(1) Provides advice and other assistance to the PBGC Director, and other senior officials to ensure that information technology (IT) is acquired and information resources are managed for the agency in a manner that is consistent with the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA).

(2) Designates a Chief Information Security Officer (CISO) to execute the IT Security Program.

c. **Chief Information Security Officer (CISO).**

(1) Performs functions for the CIO as defined by FISMA.

(2) Develops, documents, and implements an agency-wide IT security program to provide information security for the information and information systems that support the operations and assets of the agency.

(3) Develops and maintains information security policies, procedures, and control techniques to address all applicable requirements for protecting sensitive information.

(4) Assists senior PBGC officials in carrying out their information security responsibilities.

(5) Serves as the CIO's primary liaison to Information System Owners with respect to IT security issues and concerns, including those involving PII.

(6) Provides mandatory computer security training for PBGC employees and contractors, at the time of hiring/onboarding and on an annual basis, to make them aware of the policies and procedures for protecting sensitive information.

d. **Senior Agency Official for Privacy (SAOP).**

(1) Ensures implementation of information privacy protections, including full compliance with laws, regulations and policies relating to information privacy, such as the Privacy Act.

(2) Participates in agency information privacy compliance activities (i.e., privacy policy as well as information policy).

(3) Participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals.

(4) Participates in assessing the impact of technology on the privacy of personal information.

(5) Reviews privacy procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and Federal guidance.

(6) Consults and collaborates with the appropriate PBGC departments in identifying, developing, adopting, and implementing, as needed, additional or revised privacy procedures.

(7) Ensures that employees and contractors receive appropriate training and education regarding their privacy protection responsibilities.

(8) Prepares and submits various privacy-related reports, such as the annual Senior Agency Official Privacy Report to OMB required by FISMA.

(9) Works closely with the CIO and CISO to reduce the exposure of PII in PBGC information systems and in the conduct of PBGC business, and to reduce the holdings of PII whenever possible.

e. **Chief Privacy Officer (CPO).**

(1) Initiates, facilitates, and promotes activities to foster information privacy awareness within PBGC, especially with regard to sensitive information.

(2) Develops and supports privacy protection policies and procedures.

(3) Assists PBGC departments in achieving and maintaining compliance with the Privacy Act, the Freedom of Information Act (FOIA), and other relevant legal authorities.

(4) Provides guidance to PBGC departments and employees regarding privacy matters.

(5) Develops and presents training on protecting sensitive information to new hires, employees, and contractors.

(6) Provides guidance to information system owners on conducting Privacy Impact Analyses (PIAs) and Privacy Threshold Assessments (PTAs).

(7) Develops and provides guidance on drafting and maintaining accurate System of Records Notices (SORNs).

(8) Receives and responds to questions and concerns regarding PBGC's privacy policies and procedures.

(9) Receives, documents, tracks, and addresses all suspected and confirmed privacy breaches, including reporting to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) when required, and notifying impacted individuals when appropriate.

f. **General Counsel.**

(1) Provides legal advice about the policies and procedures to protect sensitive information.

(2) Provides legal advice about the Privacy Act, the FOIA, and other relevant legal authorities.

(3) Assists the SAOP and CPO in performing their duties as needed.

(4) Works closely with the CIO to minimize the risk of loss, unauthorized access, or other misuse of sensitive information.

g. **Disclosure Officer.**

(1) Establishes and administers a process for receiving, documenting, tracking, and responding to requests for information under FOIA and the Privacy Act.

(2) Ensures procedures are in place to manage and prevent inappropriate release of sensitive information in response to requests for information under FOIA or the Privacy Act.

(3) Provides FOIA training for PBGC employees and contractors.

h. **Workplace Solutions Department Director.**

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

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

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

i. **Information Owner (IO).**

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

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

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

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

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

(3) Ensures the information system is operated according to the agreed upon security requirements.
(4) Ensures that adequate security measures and procedures are implemented to protect the data residing on their system(s).

k. **Information System Security Officer (ISSO).**
(1) Acts as a liaison between the business unit and WSD for physical security, and IT Infrastructure Operations Department for logical access.
(2) Communicating directives, policy and guidance to their business unit and relaying issues to the appropriate parties.
(3) Ensures work products and documents are properly labeled and maintained according to privacy and records management requirements.
(4) Evaluates compliance with agency information security policies, procedures, and control techniques to protect sensitive information within their assigned business area.

l. **Procurement Director.**
(1) Ensures that all contracts and other agreements include provisions requiring contractors and subcontractors to follow PBGC's policies and procedures for protecting sensitive information.
(2) Initiates appropriate corrective action against a contractor for failure to follow PBGC's policies and procedures for protecting sensitive information.
(3) Through CORs, ensures that contractors successfully perform the responsibilities detailed in section m. below.

m. **Office of Policy and External Affairs (OPEA).**
(1) Oversees and directs outreach to PBGC external stakeholders, including the press.
(2) Interacts with the Congress, Executive Branch agencies, and industry and labor groups on ERISA and PBGC issues.
(3) Coordinates legal advice, analysis, research, and recommendations for the development of policy, regulations and legislation.
(4) Coordinates with Disclosure Division (in the Office of General Counsel) when responding to requests for sensitive information from the media or Congress, and when there are questions regarding whether information is sensitive.

n. **Supervisors and managers.**
(1) Instruct employees and contractors of their responsibilities to protect sensitive information.
(2) Ensure employees and contractors attend all required or mandatory training related to protecting privacy or sensitive information.
(3) Initiate corrective or disciplinary action when an employee or contractor fails to follow PBGC's policies and procedures for protecting sensitive information.

o. **Employees and contractors.**
(1) Be diligent about protecting sensitive information.

(2) Adhere to the policies and procedures established by PBGC to protect sensitive information, whether in electronic or hard copy format, used while performing official duties.
(3) Satisfactorily complete mandatory training related to protecting privacy or sensitive information.
(4) Seek guidance from their supervisor or COR, as appropriate, if they have any questions on how to protect sensitive information.
(5) Immediately report any suspected or confirmed privacy breaches to Privacy_Breach@pbgc.gov, the SAOP, or the Chief Privacy Officer (including the loss of control or unauthorized disclosure of sensitive information, which must be reported to US-CERT by the Chief Privacy Officer within one hour of discovery).

9. PROCEDURES:

a. **Physical, Technical and Administrative Safeguards.**

(1) PBGC employs a variety of physical, technical, and administrative safeguards to protect sensitive information.
(2) PBGC protects sensitive information by using physical safeguards including, but not limited to:
   i. Requiring employees and contractors to wear a PBGC-issued photo identification or Interim ID/Access badge (compliant with HSPD-12) at all times, limiting access to PBGC's offices to individuals with proper identification, and requiring visitors and guests to be signed in and escorted through the building at all times.
   ii. Key control management and limiting access within PBGC's offices to authorized individuals (i.e., individuals with PBGC-issued photo identification cards), including additional limitations based on the time of day, day of week, and the individual's official duties.
   iii. Requiring employees and contractors (with offices that can be locked) to lock their office doors whenever they vacate their offices.
   iv. Storing information in locked filing cabinets and file rooms.
(3) PBGC protects sensitive information by using technical safeguards including, but not limited to:
   i. Use of security monitoring tools, data loss prevention tools, antivirus programs, firewalls, and malware detection applications.
   ii. Host and network-based intrusion detection systems.
   iii. Host and network-based intrusion prevention systems.
   iv. Connection encryption schemes, including a virtual private network.
   v. Strong email and device encryption.
   vi. Regular data back-ups.
   vii. Requiring two-factor authentication to access PBGC's networks.

(4) PBGC protects sensitive information by using administrative safeguards including, but not limited to:

i. Consistently emphasizing that protecting individuals' privacy and the confidentiality of non-public information is critically important to the success of PBGC, and fostering an environment where privacy and confidentiality considerations are always given proper attention.

ii. Requiring all employees and contractors to complete privacy and security training prior to being given access to PBGC's networks and information.

iii. Requiring all employees and contractors to complete an annual privacy refresher training course, and offering additional targeted trainings on an as-needed basis.

iv. Issuing privacy-related reminders and guidance on an as-needed basis, including issuing guidance about identifying and protecting sensitive information:

1. In the office, and while traveling or teleworking;
2. On mobile devices; and
3. While using shared drives, including SharePoint.

v. Counseling and disciplining individuals or departments as needed.

b. **Handling Federal Tax Information.**

(1) Federal tax information ("FTI") is any Federal tax return or return information received from the Internal Revenue Service ("IRS") or a secondary source, such as the Social Security Administration, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. FTI includes any information created by the recipient that is derived from Federal return or return information.

(2) IRS regulations require that additional safeguarding measures be taken to protect FTI.

(3) PBGC Directive IM 10-2, *Safeguarding Federal Tax Information Disclosed to the PBGC under Section 6103 of the Internal Revenue Code*, governs employee access to Federal tax returns and return information from the IRS.

c. **Responding to Requests for Sensitive Information.**

(1) PBGC routinely receives requests for sensitive and non-sensitive information from a variety of sources including, but not limited to, PBGC current and former employees, participants in pension plans insured or trusteed by PBGC, attorneys representing participants or their beneficiaries, students and professors studying ERISA, non-profit organizations, public interest groups, the media, and Congress.

(2) The Disclosure Division in the Office of General Counsel is responsible for handling all requests for information subject to the FOIA and the Privacy Act.

(3) The Office of Policy and External Affairs (OPEA) oversees and directs outreach to PBGC external stakeholders, including the press; interacts with Congress, Executive Branch agencies, and industry and labor groups

on ERISA and PBGC issues; and coordinates legal advice, analysis, research, and recommendations for the development of policy, regulations and legislation.

(4) The Disclosure Division and OPEA coordinate when responding to requests for sensitive information from the media or Congress, and when there are questions regarding whether information is sensitive.

(5) PBGC employees and contractors must refer all third-party requests for access to or copies of sensitive information to the Disclosure Division for processing under the FOIA and the Privacy Act.

d. **Privacy Breach Reporting.**

(1) PBGC defines a privacy breach as loss of control, compromise, unauthorized disclosure, acquisition, or access, or any similar situation involving an other than authorized purpose where persons other than authorized users have access or potential access to PII, whether physical or electronic.

i. Examples of privacy breaches:

1. Emailing unencrypted documents with PII to a personal e-mail account.
2. Accidentally emailing sensitive information to your friend that you meant to email to a co-worker.
3. Sending a benefit determination letter to someone other than the intended recipient.
4. Leaving paperwork containing sensitive information on the metro.
5. Disposing of paperwork containing sensitive information in a trash can rather than a secured shred bin.
6. Storing documents containing sensitive information on a shared drive that may be accessed by persons who do not have an official 'need-to-know'.
7. Losing your smartphone.

(2) It is the responsibility of all PBGC employees and contractors to safeguard all sensitive information that is in his/her possession or to which he/she has access.

(3) Any PBGC employee or contractor employee who discovers or otherwise learns of a suspected or actual breach, whether electronic or physical, must immediately report it to Privacy_Breach@pbgc.gov, the SAOP, or the Chief Privacy Officer.

(4) The Chief Privacy Officer is responsible for ensuring that all actual or suspected privacy breaches are cataloged and timely reported to US-CERT when appropriate.

(5) The procedures contained in PBGC's Breach of Personally Identifiable Information Notification Policy and Procedures, as well as other internal memoranda issued by the SAOP or the Chief Privacy Officer (as frequently as needed to stay in compliance with FISMA and OMB guidance) should be followed to the greatest extent possible. If unforeseen circumstances occur that make following such procedures impractical,

inefficient, or otherwise inadequate, adjustments may be made, but PBGC's "best judgment" standard (adopted pursuant to OMB M-07-16) should remain the guiding principle at all times.

e. **Security Incidents.**

(1) A security incident is computer-based or network-based activity which results (or may result) in misuse, damage, denial of service — including viruses, compromise of integrity, or loss of confidentiality of a network, computer, application, or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

(2) Any PBGC employee or contractor employee who discovers or otherwise learns of a security incident must immediately report it to the OIT Service Desk, by calling (202) 326-4000 ext. 3999, or emailing Desk.Service@pbgc.gov.

f. **Data Masking and Using Artificial Data.**

PBGC understands the need to avoid using sensitive information, including PII, for release development, release testing, or production support purposes. When possible, artificial data is to be used for these purposes. If artificial data is not available, sensitive data will be masked. A Plan of Action and Milestones (POA&M) will be used to track work leading to the elimination of unmasked sensitive data in all non-production environments. If the use of unmasked data in non-production environments will not be remediated, the authorizing official(s) of the system(s) using such data will complete risk acceptance forms.

10. MISCONDUCT AND CORRECTIVE ACTION:

a. Misconduct for which PBGC may initiate corrective, disciplinary, and/or adverse action includes, but is not limited to:

(1) Failing to follow the policies or procedures established to protect sensitive information, including PII, regardless of whether that failure resulted in the loss or unauthorized disclosure of sensitive information.

(2) Accessing without authorization, exceeding authorized access to, or unauthorized disclosure of, sensitive information.

(3) Failing to report a known or suspected loss of control or unauthorized disclosure of sensitive information.

(4) For supervisors and managers, failing to adequately instruct, train, or supervise employees in their responsibilities to protect sensitive information, including PII.

b. Failure to protect sensitive information may also constitute a violation of one or more the following Federal laws, which contain civil and/or criminal penalties:

(1) The Privacy Act.
(2) The Trade Secrets Act.
(3) The Internal Revenue Code.
(4) The Computer Fraud and Abuse Act.
(5) The Procurement Integrity Act.

c. PBGC may take corrective action against employees and contractors who fail to protect sensitive information including, but not limited to:

(1) Removal of an individual's authority to access PBGC information systems.

(2) Employee discipline under PBGC Directive PM 30-1, *Disciplinary and Adverse Actions*.

(3) Contractor suspension or debarment under PBGC Directive FM 15-3, *Suspension and Debarment Program*.

(4) Seeking damages under applicable contract law.

d. Legal actions that may result in legal or criminal penalties may also be initiated by third parties including, but not limited to, the Office of Inspector General, the Department of Justice, and individuals harmed by an employee's or contractor's action/inaction.