Pension Benefit Guaranty Corporation

Directive

Subject: Protecting Personally Identifiable Information

Directive Number: IM 10-03

Originator: OGC

ALICE MARONI

Digitally signed by ALICE MARONI
Date: 2024.09.25 10:29:13 -04'00'

Alice C. Maroni
Chief Management Officer

1. **PURPOSE:** This Directive establishes the policies and procedures for protecting Personally Identifiable Information (PII).

2. **EFFECTIVE DATE:** This Directive replaces and supersedes the Pension Benefit Guaranty Corporation's (PBGC) Directive IM 10-3 dated 10/30/2015 and is effective on the date shown above.

3. **SCOPE:** This Directive applies to all PBGC federal employees and contractors, as well as any other persons who have access to PII used in the performance of PBGC business, and to all PBGC IT systems and processes, and any federal information system operated on behalf of PBGC which collects, processes, maintains, uses, shares, disseminates, or disposes of PII.

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. Internal Revenue Code, I.R.C. § 6103, *Confidentiality and Disclosure of Returns and Return Information*.
   e. Internal Revenue Code, I.R.C. § 7213, *Unauthorized Disclosure of Information*.
   f. Clinger-Cohen Act, 40 U.S.C. §§ 1401 *et seq.*
   g. Paperwork Reduction Act, 44 U.S.C. §§ 3501-3521.
   h. E-Government Act of 2002, U.S.C. § 101 *et seq.*
   i. Federal Information Security Modernization Act of 2014, 44 U.S.C. §§ 3541 *et seq.*
   j. Foundations for Evidence-Based Policymaking Act of 2018
   k. Management and Promotion of Electronic Government Services, 44 U.S.C. §§ 3601-3606.
   l. Exec. Order 13556, 75 Fed. Reg. 68675, *Controlled Unclassified Information* (Nov. 4, 2010); 32 C.F.R. Part 2002.
   m. Federal Information Processing Standard Publication 140-2 (until 2026; thereafter Federal Information Processing Standard Publication 140-3).

n. Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors* (Aug. 27, 2004).
o. Office of Management and Business (OMB) Circular A-130, *Management of Federal Information Resources* (July 28, 2016).
p. OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (Sept. 30, 2003).
q. OMB Memorandum M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (Sept. 15, 2016).
r. OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017).
s. PBGC Directive FM 15-03, *Suspension and Debarment Program*.
t. PBGC Directive IM 05-02, *PBGC Information Security Policy*.
u. PBGC Directive IM 05-04, *Use of Information Technology Resources*.
v. PBGC Directive IM 05-09, *PBGC Privacy Program*.
w. PBGC Directive IM 10-02, *Safeguarding Federal Tax Information Disclosed to the Pension Benefit Guaranty Corporation under Section 6103 of the Internal Revenue Code*.
x. PBGC Directive IM 10-07, *Controlled Unclassified Information*.
y. PBGC Directive IM 15-03, *PBGC Records Management Program*.
z. PBGC Directive PM 30-01, *Disciplinary and Adverse Actions*.
aa. PBGC Office of Information Technology Glossary of Terms.
bb. PBGC Privacy Breach Response Plan.
cc. PBGC Security Incident Management Plan.

5. **BACKGROUND:** This Directive establishes PBGC's policies to protect PII held by or on behalf of PBGC (by another federal agency or a contractor). PII held by PBGC, or on its behalf, requires protection from loss, misuse, and Unauthorized Access or modification. A failure to protect this information may result in a violation of the law, penalties levied against PBGC or the individual responsible for the violation, and in avoidable costs or damage to the PBGC's reputation.

6. **DEFINITIONS:**
a. **Authorizing Official**. Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

b. **Breach**. A 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 personally identifiable information or (2) an authorized-user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

c. **Business Executive**. For systems that have been consolidated into the Information Technology Infrastructure Services General Support System (GSS), the PBGC executive who is responsible for with a significant role in establishing

organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations.

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

e. **Control**. The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. Administrative controls define the human factors of security and involve all levels of personnel within an organization, determining which users have access to what resources and information. Physical controls are security measures in a defined structure used to deter or prevent Unauthorized Access to PII or Information Systems. Technical controls use technology as a basis for controlling the access and usage of PII throughout a physical structure and over the network.

f. **Controlled Unclassified Information (CUI)**. Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does <u>not</u> include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

g. **Information Owner (IO)**. For systems that have not been consolidated into the GSS, the PBGC official with statutory or operational authority for specified information and the responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
For systems consolidated into the GSS, the PBGC official of the department or organization that owns the information and the mission functionality of the subsystem/child. The IO establishes policies and procedures governing generation, collection, processing, dissemination, and disposal of information.

h. **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.

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

j. **Information System Owner**. The PBGC official responsible for the overall procurement, development, integration, modification, security and operation and maintenance of an Information System.

k. **Need-to-know**. 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."

l. **Person**: an individual, partnership, corporation, association, or public or private organization other than an agency.

m. **Personally Identifiable Information (PII)**: PII refers to 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. To determine whether information is PII, the agency shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available - in any medium or from any source - that would make it possible to identify an individual.

n. **Privacy Impact Assessment (PIA)**. An analysis of how PII 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 PII in an identifiable form in an electronic Information System, and (iii) to examine and evaluate protections and alternative processes for handling PII to mitigate potential privacy risks.

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

p. **Risk Acceptance**. The analysis of a vulnerability that is present when a control is not in place and is not planned to be remediated (and therefore is not tracked in a Plan of Action and Milestones – POA&M) or the individual, program, entity, or system cannot comply with a PBGC policy. The documentation of the analysis on the Risk Acceptance Form formalizes the Information System Owner (ISO)/Information Owner (IO) and Authorizing Official's (AO) decision to accept the risk by describing the risk in terms of confidentiality, integrity, and availability; the impact and likelihood of the risk being realized; and the compensating controls that are in place to reduce the risk to an acceptable level.

q. **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.

r. **Synthetic Data**. Data generated and/or created using algorithms and statistical models. Instead of being collected through direct measurement or real-world observations, synthetic data replicates the statistical properties and patterns of the original data. It does not contain any identifiable information of actual individuals or entities. Synthetic data facilitates analysis, testing, and development while ensuring privacy and security without the constraints associated with live data.

s. **Unauthorized Access**. A Person gains logical or physical access without permission to a network, system, application, data, or other resource.

7. **POLICY:** It is PBGC's policy to protect the confidentiality, integrity, and availability of PII from Unauthorized Access and disclosure by properly safeguarding, disseminating, and destroying such information in accordance with applicable laws and regulations. PBGC shall:

a. Encrypt PII stored on PBGC-issued IT equipment (e.g., laptop and desktop computers), contractor IT equipment, and removable media (e.g., USB flash drives).

b. Avoid using PII for release development, release testing, training, or production support purposes. Synthetic Data must be used for these purposes. Use of production PII data is only allowed as an exception when synthetic data is either not available or not practical and must be documented using the Policy Deviation procedure and summarizing the specific system development requirements that necessitate use of production data, whether the data will be masked and, if not, why it cannot be masked, and an alternative to safeguard the data/information. The Risk Acceptance must be approved by the Privacy Office, the CISO, the Information Owner, the Authorizing Official, and the ITIOD Director (if different than the Authorizing Official).

Common Control Providers, Information System Owners, and Information Owners shall:

a. Implement the applicable physical, administrative, and technical Controls necessary to protect PII from Unauthorized Access or disclosure.
b. Document the remediation of applicable Controls that are assessed as "Other than Satisfied" in a Plan for Action and Milestones (POA&M) or, in the event remediation is not possible, document the reason and compensating controls in a Risk Acceptance.

All PBGC employees and contractors are responsible for protecting PII and those granted access to PBGC data shall:

a. Collect, maintain, and disseminate PII only when it is necessary to satisfy a PBGC business need;

b. Use PII only in a way that is compatible with the purpose for which it was collected;

c. Protect PII from Unauthorized Access and disclosure. Only those individuals who have a Need-to-know in the performance of their duties shall be provided access to PII;

d. Conduct PBGC business only on networks or accounts operated by PBGC or on behalf of PBGC;

e. Obtain approval prior to the removal of PII from PBGC IT devices/network, contractor devices/network, or the workplace. Approval must obtained from the Chief Privacy Officer for the proposed removal of PII and from the CUI Program Manager for all other CUI (see PBGC Directive IM 10-7);

f. Print PII in accordance with PBGC's printing policy;

g. Access PII stored in electronic format only across a secure PBGC connection;

h. Disseminate PII outside of PBGC only when required and, when done electronically, use a PBGC-approved data encryption method or a secure file transfer application;

i. Properly dispose of electronic media and paper documents containing PII when they are no longer needed in accordance with PBGC Directive IM 15-03, PBGC's Records Management Program and PBGC Directive IM 10-07, Controlled Unclassified Information Program;

j. Complete mandatory Annual Cyber Awareness Training; and,

k. Comply with the procedures, processes, and guidance developed and disseminated under this Directive.

8. **POLICY DEVIATIONS:**

a. The Senior Agency Official for Privacy (SAOP) and Chief Information Security Officer (CISO) have the authority to approve a policy deviation. Requests for a deviation from a policy must come from a Department Director or higher and be documented with the PBGC's Risk Acceptance Form.

NOTE: For the process to seek a CUI Waiver or Challenge, see PBGC Directive IM 10-7.

b. Documentation of the request and adjudication of the request shall be maintained in Cyber Security Assessment and Management (CSAM) system.

c. Approved policy deviations shall be reviewed at least annually.

d. Any change in the underlying risks that led to the approved policy deviation should be reported to the SAOP and CISO 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 under this Directive, shall be subject to:
   (1) PBGC Directive PM 30-01, for employees.
   (2) PBGC Directive FM 15-03, for contractors.

b. Individuals will be denied access to PBGC Information Systems and PII.

c. Failure to protect PII 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 Internal Revenue Code.
   (3) The Computer Fraud and Abuse Act.

10. **RESPONSIBILITIES:**

a. **PBGC Director.**
   (1) Retains overall responsibility for protecting PII.
   (2) Hires the Chief Information Officer (CIO).
   (3) Appoints the Senior Agency Official for Privacy (SAOP).
   (4) Appoints the Senior Agency Official for CUI (SAO-CUI).
   (5) Ensures policies are developed and implemented to mitigate the risk to PBGC's operations, assets, and the individuals it serves.

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 Modernization Act (FISMA).
   (2) Designates a Chief Information Security Officer (CISO) to execute the IT Security Program.
   (3) Ensures development and implementation of policies to establish PBGC's commitment to Information Security and the actions required to effectively manage risk and protect the core missions and business functions performed

by PBGC.

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

(1) The CISO develops, documents, and implements an agency-wide Information Security program including system and security Controls related to the protection of PII residing on or being transmitted through Information Systems that support the operations and assets of the agency.
(2) Ensures the delivery of mandatory IT 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 PII.
(3) Reviews and adjudicates policy deviation requests.

d. **Chief Data Officer (CDO).**

Coordinates with the CPO regarding PBGC's compliance with the Evidence-Based Policymaking Act of 2018 and the protection of PII maintained by PBGC.

e. **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) Provides 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) Designates a Chief Privacy Officer (CPO).
(3) Reviews the organization's privacy procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and Federal guidance.
(4) Consults and collaborates with the appropriate PBGC offices in developing, adopting, and implementing additional procedures, as needed.
(5) Ensures PBGC employees and contractors receive appropriate training and education regarding their privacy protection responsibilities.
(6) Plays a central policymaking role in the organization's development and evalu ation of
legislative, regulatory, and related policy proposals implicating privacy issues.
(7) Determines whether the Breach Response Team (BRT) should be convened.
(8) Chairs the BRT for Breaches not involving Information Systems and co-chairing the BRT with the Chief Information Security Officer (CISO) for Breaches involving Information Systems.
(9) Reviews and adjudicates policy deviation requests.
(10) Works closely with the CISO and OIT which have Information System securit y responsibilities.

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

(1) Initiates, facilitates, and promotes activities to foster privacy awareness within

PBGC.

(2) Develops and supports privacy protection policies and procedures.
(3) Assists PBGC departments in achieving and maintaining compliance with the Privacy Act and other relevant legal authorities.
(4) Coordinates with the SAO-CUI and CUI Program Manager.
(5) Provides guidance to PBGC departments and employees regarding privacy matters.
(6) Receives and responds to questions and concerns regarding PBGC's privacy policies and procedures.
(7) Receives, documents, tracks, and addresses all suspected and confirmed 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.

g. **Senior Agency Official for CUI (SAO-CUI).**
The SAO-CUI is primarily responsible for the PBGC's CUI policy and exercises a central role in overseeing, coordinating, and facilitating the organization's compliance efforts with the CUI Program. This role includes:

(1) Provides guidance to the PBGC Director and senior leadership to ensure that CUI is safeguarded in a manner in compliance with applicable federal, CUI EA, and NIST guidance.
(2) Designates a CUI Program Manager.
(3) Reviews the organization's CUI procedures to ensure they are comprehensive, current, and compliant with applicable laws and Federal guidance.
(4) Consults and collaborates with the appropriate PBGC offices in developing, adopting, and implementing newly identified and revised procedures.
(5) Ensures PBGC federal employees and contractors receive appropriate training and education regarding their CUI safeguarding responsibilities.
(6) Coordinates with the SAOP, CISO and CIO to respond to CUI incidents involving federal information systems which are determined to cause grievous harm to the agency or the individuals it serves.
(7) Reviews and adjudicates deviations from CUI policies.
(8) Works closely with the CISO and CIO who have Information System security responsibilities.

h. **CUI Program Manager.**
(1) Implements CUI guidance, training, coordination with Contracting Officers, and technology requirements.
(2) Performs PBGC's agency-wide self-inspection to ensure ongoing compliance with National Archives and Records Administration (NARA) requirements.
(3) Identifies and designates the appropriate markings for safeguarding CUI in accordance with the CUI EA's guidance.
(4) Notifies the Contracting Officer Representative (COR) when a contractor fails to follow PBGC's policies and procedures for protecting and handling CUI.

(5) Notifies the federal manager or supervisor when a federal employee fails to follow PBGC's policies and procedures for handling CUI.
(6) Ensures the agency has policies, guidance, and supporting processes to fully implement the CUI Program.
(7) Implements a mandatory CUI training program.
(8) Oversees and manages the program, waiver process, and reporting of activities related to CUI.
(9) Develops and implements a CUI self-inspection program
(10) Complies with necessary CUI training requirements
(11) Develops and maintains the CUI Program's policies, procedures, processes, training, and Controls to address all requirements set forth in federal law, regulations, and guidance.
(12) Serves as the PBGC lead in investigating reported incidents involving CUI, except for the reporting of cybersecurity and insider threat incidents and PII breaches.
(13) Keeps SAO-CUI, SAOP, CIO, and CISO advised of CUI activities, as necessary.
(14) Executes PBGC's compliance assessment activities to ensure ongoing compliance with applicable laws, regulations, and federal guidance.

i. **Common Control Provider.**
A Common Control Provider is an organization within PBGC that offers security or privacy controls for inheritance by information systems.
(1) Oversees the development, implementation, assessment, risk management, authorization and monitoring of common controls.
(2) Ensures that required assessments of common controls are performed by qualified assessors with an appropriate level of independence defined by the organization.
(3) Documents and addresses common control weaknesses or deficiencies.

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. **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 PII in response to requests for information under FOIA or the Privacy Act.
(3) Provides FOIA training for PBGC employees.

k. **Business Executive.**
For systems that **have** been consolidated into the ITISGSS boundary:
(1) Senior official or executive with specific mission responsibility and that has a security or privacy interest in the organizational systems supporting those missions.

(2) Key stakeholder with a significant role in establishing organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations.
(3) Appoints Information Owners as needed.
(4) Escalates any disputed matter to C-level executive for the business area.
(5) Appointed by the C-level executive for the business area.

l. **Information Owner (IO)/Information System Owner (ISO).**
For systems that have **not** been consolidated into the ITISGSS boundary:
(1) Safeguards the information contained in the system in which it resides, whether or not it resides at PBGC.
(2) Involves the CUI Program, privacy, and cybersecurity in IT System Lifecyle Management activities.
(3) Ensures the inclusion of all applicable contract clauses when procuring service or systems that will collect, maintain, or disseminate PII.

m. **Information Owner (IO).**
For systems that **have** been consolidated into the ITISGSS, the IO is a Federal employee of the PBGC department or organization that owns the information and the mission functionality of the subsystem or child. The IO:
(1) Establishes policies and procedures governing generation, collection, processing, dissemination, and disposal of information.
(2) Safeguards the information contained in the assigned subsystem or child and retains that responsibility when information is shared with or provided to other organizations.
(3) Ensures that solicitation requirements for professional IT services have the appropriate references and clauses needed to address information security in the final solicitation package.
(4) Works with the ISSPO to ensure compliance with information security requirements and support system authorization.
(5) Appointed by the Business Executive.
(6) Appoints the Service/Application Owners.
(7) Escalates any disputed matter to the Business Executive.
(8) Serve as a member of the IO Council.

n. **Information System Security Privacy Officer (ISSPO).**
(1) Acts as a liaison between the business unit and Common Control Providers.
(2) Communicates directives, policies and guidance to their business unit and relays issues to the appropriate parties.
(3) Ensures work products and documents are properly labeled and maintained according to CUI and records management requirements.
(4) Evaluates compliance with agency Information Security and privacy policies, procedures, and control techniques to protect PII within their assigned business area.

m. **Service/Application Owner.**
For systems that **have** been consolidated into the ITISGSS, a Service/Application Owner is the Federal employee of the PBGC department or organization that owns the information and the mission functionality of the subsystem or child.
(1) Manages access to the service/application information and approves access requests.
(2) Serves as the subject matter expert (SME) and mission functionality of the service or application.
(3) Coordinates and approves IT service/application changes.

n. **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 PII.
(2) Initiates appropriate corrective action against a contractor for failure to follow PBGC's policies and procedures for protecting PII.

o. **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 PII from the media, Congress, the White House, and when there are questions regarding whether information constitutes PII.

p. **Supervisors/CORs.**
(1) Instruct employees and contractors of their responsibilities to protect PII.
(2) Ensure employees and contractors attend all required or mandatory training related to protecting privacy or PII.
(3) Initiate disciplinary action when an employee fails to follow PBGC's policies and procedures for protecting PII. Initiate a conversation with the Procurement Department when a contractor fails to follow PBGC's policies and procedures.

q. **Employees and contractors.**
(1) Diligently protect PII.
(2) Adhere to the policies and procedures established by PBGC to protect PII, whether in electronic or hard copy format, used while performing official duties.
(3) Satisfactorily complete mandatory Cyber Awareness training related to protecting privacy or other CUI.
(4) Submit written requests for the removal of PII from the workplace to the CPO or their designee.

(5) Seek guidance from the Privacy Office, as appropriate, if they have any questions on how to protect PII.
(6) Immediately report any suspected or confirmed Breaches using the Reportal found on the Intranet Homepage under Quick Links.
(7) Immediately report a Security Incident using the Reportal found on the Intranet Homepage under Quick Links or to the OIT Service Desk, by calling (202) 326-4000 ext. 3999
(8) Immediately report any suspected incident involving CUI that does not contain PII using the Reportal found on the Intranet Homepage under Quick Links.