Pension Benefit Guaranty Corporation

Directive

Subject: Controlled Unclassified Information Program

Directive Number: IM 10-07

Originator: OMA

ARRIE ETHERIDGE Digitally signed by ARRIE ETHERIDGE Date: 2025.10.27 15:36:50 -04'00'

Arrie Etheridge
Acting Chief Management Officer

1. **PURPOSE:** This Directive establishes the Pension Benefit Guaranty Corporation's (PBGC) Controlled Unclassified Information (CUI) program, the framework for managing this program, and responsibilities for protecting CUI in accordance with 32 C.F.R. Part 2002, the CUI Executive Agent (CUI EA), and the National Institute of Standards and Technology (NIST).

2. **EFFECTIVE DATE:** This Directive is effective as of the date noted above.

3. **SCOPE:** This Directive applies to all PBGC federal employees and contractors PBGC IT systems and processes, and any federal information system operated on behalf of PBGC which collects, processes, maintains, uses, shares, disseminates, transmits, or disposes of CUI.

4. **AUTHORITIES:**
   a. Executive Order 13556, 75 Fed. Reg. 68675, *Controlled Unclassified Information (CUI)*
   b. 32 C.F.R. Part 2002, *Controlled Unclassified Information*
   c. FAR Clause 52-204-21, *Basic Safeguarding of Covered Contractor Information Systems*
   d. 5 U.S.C. § 552, *Freedom of Information Act*
   e. 5 U.S.C. § 552a, *The Privacy Act of 1974*
   f. NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*
   g. NIST Special Publication 800-60, volume 1 & volume 2, *Information Security*
   h. NIST Special Publication 800-88, *Guidelines for Media Sanitization*
   i. NIST Special Publication 800-171, *Protecting CUI in Nonfederal Information Systems and Organizations*
   j. NIST Special Publication 800-171A, *Assessing Security Requirements for Controlled Unclassified Information*
   k. NIST Special Publication 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information*

l. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*
m. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*
n. *Federal Information Security Modernization Act of 2014* (FISMA), as amended, 44 U.S.C. Chapter 35
o. PBGC Directive IM 05-02, *PBGC Information Security Policy*
p. PBGC Directive IM 05-04, *Use of Information Technology Resources*
q. PBGC Directive IM 05-09, *PBGC Privacy Program*
r. PBGC Directive IM 10-02, *Safeguarding Tax Return Information*
s. PBGC Directive IM 10-03, *Protecting Personally Identifiable Information*
t. PBGC Directive FM 15-03, *Suspension and Debarment Program*
u. PBGC Directive PM 30-01, *Disciplinary and Adverse Actions*
v. PBGC Risk Management Framework

5. **BACKGROUND:** On November 4, 2010, the President signed Executive Order (E.O.) 13556, *Controlled Unclassified Information*. The Order established a government-wide CUI Program initiative to standardize the way the executive branch handles unclassified, but sensitive, information and mandated executive agencies to establish a program to identify and protect CUI in accordance with applicable laws, regulations, and government-wide policies. The National Archives and Records Administration's (NARA's) Information Security Oversight Office (ISOO) serves as Executive Agent (EA) and established a CUI Registry of authorized CUI categories and appropriate markings.

The CUI regulations in 32 C.F.R. Part 2002 implement E.O. 13556 and establish CUI Program requirements for protecting, disseminating, marking, decontrolling, and disposing of CUI.

6. **POLICY:** PBGC requires all PBGC federal employees and contractors to comply with the policies set forth in this Directive to protect data and information designated as CUI until authorized for public release through an official PBGC release process.

a. PBGC shall identify CUI using only the categories documented in NARA's CUI Registry.

b. PBGC will not identify data or information as CUI to conceal illegality, negligence, ineptitude, or other disreputable circumstances embarrassing to any individual, agency, the federal government, or any of their partners, or for any purpose other than to adhere to the law, regulation, or government-wide policy authorizing the control.

c. PBGC shall protect all CUI, marked or unmarked, through physical, administrative, and technical controls to prevent and/or detect unauthorized access.
d. All PBGC federal employees and contractors with access or potential access to CUI are held accountable for knowing and understanding CUI handling and protection procedures outlined in this policy and disseminated via mandatory training or program guidance.

e. All information-systems which collect, process, maintain, use, share, disseminate, transmit, or dispose of CUI shall be marked and protected according to applicable laws, regulations, and government-wide policies to minimize the risk of unauthorized disclosure while allowing access by authorized holders.

f. *Federal* information systems which collect, process, maintain, use, share, disseminate, transmit, or dispose of CUI shall be categorized at the moderate confidentiality impact level in accordance with Federal Information Processing Standard 199, Standards for Security (FIPS Publication 199). Federal information systems which collect, process, maintain, use, share, disseminate, transmit, or dispose of CUI must incorporate the security requirements and controls to protect CUI at the moderate confidentiality impact level into their design and operation. *Nonfederal* systems must meet the standards in the NIST SP 800-171, when established by contract.

g. CUI may be shared to further an authorized, lawful government purpose. CUI disseminated to those outside PBGC is completed through appropriate agreements or arrangements to ensure proper protection and must be marked with Standard CUI Markings.

h. All entities within scope of this Directive comply with the procedures, processes, and guidance developed and disseminated by the CUI Program via the Controlled Unclassified Information (CUI) Program Intranet page, email, or any other methods to address CUI 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.

7. **RESPONSIBILITIES:**

a. **PBGC Director.**
   (1) Retains overall responsibility and accountability for protecting CUI commensurate with the degree of risk and level of harm to PBGC's operations.
   (2) Appoints a CUI SAO in writing.
   (3) Approves agency policies, as required, to implement PBGC's CUI Program.
   (4) Establishes and maintains a self-inspection program to ensure the agency complies with the requirements established in E.O. 13556, 32 C.F.R. 2002, and the CUI Registry.

b. **CUI Senior Agency Official (CUI SAO).** The CUI SAO is primarily responsible for the PBGC CUI policy and exercises a significant role in overseeing, coordinating, resourcing, and facilitating the organization's compliance efforts with PBGC's CUI Program.

   This role:
   (1) Serves as the primary point of contact for official correspondence,

accountability reporting, and other matters of record between the agency and the CUI EA;

(2) Serves as identification and decontrol authority for PBGC CUI.
(3) Designates PBGC-defined small groups for the purposes of this Directive.
(4) Provides guidance to the PBGC Director and senior leadership to ensure that CUI is handled and protected in a manner which complies with applicable laws, regulations, government-wide policies, and CUI EA guidance;
(5) Designates a CUI Program Manager in writing;
(6) Ensures the organization's CUI procedures are comprehensive, current, and compliant with applicable laws, regulations, government-wide policies, and federal guidance;
(7) Consults and collaborates with the appropriate PBGC offices in developing, adopting, and implementing newly identified and revised procedures;
(8) Ensures PBGC federal employees and contractors receive appropriate training and education regarding their CUI handling and protection responsibilities;
(9) Works closely with the CISO, CIO, and SAOP who have electronic information system security responsibilities;
(10) Establishes processes and criteria for reporting and investigating Misuse of CUI;
(11) Coordinates with the CISO, CIO, SAOP, and other relevant stakeholders as needed to respond to CUI Misuse events involving federal information systems which are non-compliant with this Directive;
(12) Informs other agencies if their CUI was part of PBGC's CUI Misuse event;
(13) Notifies authorized recipients, the CUI EA, and the public of any waivers granted by PBGC, including a description of all waivers in the annual report to the CUI EA, along with the rationale for each waiver and, where applicable, the alternative steps PBGC is taking to ensure sufficient protection of CUI within the agency;
(14) Establishes a mechanism by which authorized holders (both inside and outside PBGC) may contact a designated agency representative for instructions reporting the receipt of unmarked or improperly marked information the agency designated as CUI;
(15) Reviews and settles deviations from PBGC's CUI policy;
(16) Establishes a process to accept and manage CUI policy deviation requests.
(17) Develops and implements PBGC's Self-Inspection program.
(18) Takes required role-based training as applicable.
(19) The Workplace Solutions Department (WSD) manages PBGC's CUI Program. PBGC's Director has appointed the WSD Director as PBGC's CUI Senior Agency Official (CUI SAO). This role may be re-appointed to any qualified Senior Agency Official in the future.

c. **CUI Program Manager.** The CUI Program Manager is primarily responsible for daily operations of PBGC's CUI Program and implementing PBGC's CUI policy, procedures, and compliance efforts.

This role includes:

(1) Developing and maintaining PBGC's CUI Program's policies, procedures, processes, training, and controls to address all requirements set forth in federal law, regulations, and guidance;
(2) Overseeing and managing the program, processes, and reporting of activities related to CUI;
(3) Identifying and designating the appropriate markings for protecting CUI in accordance with the CUI EA's guidance;
(4) Implementing a mandatory CUI training program;
(5) Assisting PBGC departments in achieving and maintaining compliance with PBGC's CUI Program and other relevant legal authorities;
(6) Partnering with the Chief Privacy Officer (CPO) to protect CUI in all formats;
(7) Identifying, developing, and/or implementing appropriate controls to protect PBGC CUI;
(8) Participating in discussions related to electronic information systems or IT processes which collect, process, maintain, use, share, disseminate, transmit, or dispose of CUI;
(9) Performing PBGC's agency-wide self-inspection to ensure ongoing compliance with NARA's CUI requirements;
(10) Receiving, documenting, tracking, and addressing all suspected and confirmed CUI Misuse events, except for the reporting of cybersecurity, insider threat incidents, and PII breaches;
(11) Notifying the Contracting Officer Representative (COR) when a contractor fails to follow PBGC's policies and procedures for protecting and handling CUI;
(12) Notifying the federal manager or supervisor when a federal employee fails to follow PBGC's policies and procedures for handling CUI;
(13) Keeping CUI SAO, SAOP, and CISO advised of PBGC's CUI program activities, as necessary;
(14) Receiving and responding to questions and concerns regarding PBGC's CUI policies and procedures.
(15) Takes required role-based training as applicable

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

This role includes:

(1) Overseeing CUI metadata tagging standards, consistent with federal data tagging approaches in accordance with the National Strategy for Information Sharing and Safeguarding, to implement marking requirements described in this Directive and PBGC's CUI Program's Guidance documents;
(2) Integrating CUI metadata tagging standards into the agency's information technology content management tools to support discovery,

access, auditing, protection, and records management decisions regarding CUI (including monitoring CUI data and information for visibility, accessibility, trust, interoperability, and comprehension);

(3) Collaborating with the CISO and CUI SAO to implement the CUI Program's CUI Misuse event response plan in the event of a situation or action involving unauthorized disclosure or misuse of CUI through PBGC's federal information systems;

(4) Working closely with the CISO, CUI SAO, and CUI Program Manager to protect CUI collected, processed, maintained, used, shared, disseminated, transmitted, or disposed of by PBGC's federal information systems.

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

The CISO develops, documents, and implements an agency-wide National Operational Security (OPSEC) and cybersecurity program which includes system and security controls related to the protection of CUI for the data, information, and federal and non-federal information systems that support the operations and assets of the agency.

This role includes:

(1) Working closely with the CUI SAO and CUI Program Manager to protect CUI collected, processed, maintained, used, shared, disseminated, transmitted, or disposed of by PBGC's federal information systems;

(2) Integrating training on protecting and handling CUI into updates to the initial and annual cybersecurity awareness training;

(3) Collaborating with the CUI SAO to implement the CUI Program's Misuse event response plan in the event of CUI Misuse event involving unauthorized disclosure or misuse of CUI through PBGC's federal information systems.

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

(1) Primarily responsible for PBGC's privacy program and exercises a significant role in overseeing, coordinating, and facilitating the organization's privacy compliance efforts.

(2) 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 of 2002, and OMB and NIST guidance.

(3) Designates a Chief Privacy Officer (CPO).

g. **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 CUI SAO and CUI Program Manager to protect CUI in all formats.

(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 Cybersecurity and Infrastructure Agency (CISA) when required, and notifying impacted individuals when appropriate.

h. **Authorizing Officials (AO), Information Security System Managers (ISSM), Information Owners (IO), and Information System Owners (ISO).**
(1) Ensure appropriate security and privacy controls are implemented for federal information systems which collect, process, maintain, use, share, disseminate, transmit, or dispose of CUI within their program areas.
(2) Ensure that adequate measures and procedures are implemented to protect the CUI data and information residing on their information system(s) from unauthorized disclosure.
(3) Ensure the federal information system is operated according to the CUI Program's requirements.
(4) Protect the CUI data and information they own and retain when the CUI data and information is disseminated to other organizations or migrated from legacy systems.

i. **Office of Policy and External Affairs (OPEA).** This office communicates with Congress, as necessary, and will communicate any public release of CUI through their official process to the CUI Program Manager.

j. **Disclosure Officer.** Establishes and administers a process for receiving, documenting, tracking, and responding to requests for information under FOIA and the Privacy Act.

k. **Contracting Officer (CO).**
(1) Ensures that solicitation requirements for IT hardware, software, and professional services have the appropriate references and clauses needed to address CUI handling and protection in the final solicitation package.
(2) Ensures appropriate clauses concerning the handling and protection of CUI are included in PBGC solicitations and contracts.

l. **Contracting Officer Representative (COR).**
(1) Provides contract management and oversight of contractor compliance with PBGC CUI policies and procedures.
(2) Ensures contractors complete all mandatory training related to the handling and protection of CUI.
(3) Promotes compliance with the CUI Program by reporting when a contractor fails to follow PBGC CUI policies and procedures to the CUI Program Manager.
(4) Ensures appropriate clauses concerning the handling and protection of CUI are included in their PBGC contracts.

m. **Office of the General Counsel (OGC).**

(1) Resolves "synchronization" issues when CUI regulations or CUI EA requirements conflict with other laws and regulations.
(2) Conducts legal sufficiency review of PBGC's CUI policies and guidance.
(3) Provides guidance to the CUI SAO when adjudicating CUI policy deviations prior to escalation to the CUI EA, as deemed necessary by the CUI SAO.

n. **Office of the Inspector General (OIG).**
In the event of an unauthorized disclosure or misuse of CUI involving a suspected criminal violation of law, rule, or regulation, takes appropriate action to mitigate risk to the agency and the individuals it serves.

o. **Agency Records Officer (ARO).** The Agency Records Officer is responsible for developing integrated records management policies to protect CUI.

This role includes:
(1) Determining if any CUI documents or materials constitute permanently valuable records of the government, which require maintenance and disposal in accordance with PBGC Directive IM 15-03, *PBGC Records Management Program*;
(2) Ensuring the continued handling and protection of CUI documents or materials when transferred and stored at offsite records storage facilities.

p. **Department Directors, Supervisors, and Managers.** All PBGC Department Directors, Supervisors, and Managers are responsible for promoting PBGC's CUI Program within their departments and divisions by:

(1) Ensuring that CUI in the department is managed and protected in accordance with this Directive, PBGC's CUI Program's Guidance documents, and PBGC's CUI Program procedures;
(2) Ensuring all employees and contractors comply with mandatory CUI training requirements;
(3) Ensuring CUI Misuse events are reported through official communication channels as instructed by PBGC's CUI Program Team;
(4) Considering corrective actions recommended by PBGC's CUI SAO or CUI Program Manager in response to a situation involving the unauthorized disclosure or Misuse of CUI;

q. **PBGC Federal Employees and Contractors**. Protecting CUI is the responsibility of every PBGC federal employee and contractor. All PBGC federal employees and contractors must:

(1) Understand their obligations with respect to handling and protecting CUI;
(2) Follow the requirements in this policy and PBGC's CUI Program's Guidance documents when handling CUI in all formats;
(3) Comply with training related to handling and protecting CUI;

(4) Report any suspected or confirmed Misuse of CUI, including the loss of control or unauthorized disclosure of CUI.

8. **DEFINITIONS:**
See Appendix A for definitions associated with the CUI Program.

9. **HANDLING/PROTECTING CUI:**
To reduce the potential of unauthorized disclosures, all PBGC federal employees and contractors shall:

a. Restrict CUI to PBGC-controlled environments to reasonably ensure that individuals without a lawful government purpose cannot access or observe CUI or overhear conversations involving CUI.
b. Secure CUI using, at minimum, physical controls when not in use.
c. Limit disseminating CUI data or information to those with an authorized, lawful government purpose. Prior to dissemination, an authorized holder of CUI must determine whether an individual has an authorized, lawful government purpose to access CUI.
d. Enter into an appropriate written agreement or arrangement with any authorized non-executive branch CUI recipient when possible. Exceptions to this rule are detailed in 32 C.F.R. 2002.16(a)(7).
e. Use encryption when emailing attachments containing CUI outside the PBGC network (sending within the PBGC network is appropriately protected). The body of the email must not contain any CUI.
f. Comply with PBGC Directive IM 05-09, *PBGC Privacy Program*, to properly protect PII entrusted to PBGC.
g. Comply with PBGC Directive IM 10-03, *Protecting Personally Identifiable Information* when collecting, processing, maintaining, using, sharing, disseminating, or disposing of PII.
h. Comply with PBGC Directive IM 10-02, *Safeguarding Tax Return Information*, to properly safeguard Federal Tax Information (FTI) (as defined in IM 10-02) entrusted to PBGC.

10. **MARKING CUI:**

a. All information systems and documents containing CUI must be marked to alert the user or recipient of the data or information's sensitive content. Details on marking and labeling CUI in various formats and for various recipients are described in PBGC's CUI Program's Guidance documents. Upon adoption of this directive, unless required by other law or regulation, Standard CUI Markings are only required when disseminating CUI outside PBGC. When disseminating CUI within PBGC and to PBGC-defined small groups (see definition above), an alternate marking method is required.

b. Use NARA's approved Limited Dissemination Markings to control groups of potential authorized recipients.

c. When disseminating PBGC CUI with authorized recipients outside PBGC, prepare the document (including email) with a Standard CUI Marking prior to dissemination. The Standard CUI Marking contains two elements:

(1) the CUI Banner Marking requires the letters "CUI" and shall replace all legacy labels when data and information are updated or re-used. This includes labels such as "For Official Use Only," "Sensitive but Unclassified," "Office Use Only", "Limited Distribution", "Pre-decisional", and any other such labels, and

(2) a CUI Designation Indicator shall include the name of the designating agency, which may take the form of official agency letterhead, signature block, or another standard agency indicator, and a point of contact (i.e., name and email) for the CUI. When feasible, the CUI Designation Indicator shall also include a decontrol date or specific event which triggers decontrol of the CUI.

d. If not utilizing the Standard CUI Markings, authorized alternate marking methods include, but are not limited to:
   (1) covering all CUI in paper format with the approved CUI cover sheet (Standard Form [SF] 901),
   (2) labeling electronic media with the appropriate authorized CUI labels (SF 902 or SF 903),
   (3) labeling storage containers and secure spaces with a noticeable sign indicating the presence of CUI,
   (4) adding metadata to electronic documents containing CUI content, or
   (5) marking electronic information systems as containing CUI upon entry or as a consistent banner markings.

e. When receiving CUI from an external source or authorized holder outside PBGC, notify the designating (originating) agency if the data or information is marked inappropriately.

f. PBGC is not authorized to modify the designating agency's CUI designation without explicit approval from the designating agency.

g. PBGC will not modify the CUI markings of another agency without explicit written consent from the designating or disseminating agency.

11. **DESTROYING CUI:**
   a. Destruction of CUI in any format must be done in a manner that renders it unreadable, indecipherable, and irrecoverable. CUI in paper format must not be disposed of in trash bins, recycling bins, or using personal office shredders. CUI in paper format must be disposed of using only PBGC-approved destruction methods.
   b. If a PBGC federal employee or contractor works from an alternate worksite, CUI must be returned to a PBGC-controlled facility for proper destruction and destroyed using PBGC-approved protocols.

12. **DECONTROLLING CUI:**
   a. There are no specific timelines to decontrol CUI unless specifically required in a law, regulation, or government-wide policy. PBGC may decontrol CUI automatically when triggered by a condition stated in 32 C.F.R. 2002.18(b) or by request of an authorized holder. PBGC may also decontrol CUI when

doing so is in the best interest of PBGC and does not conflict with governing laws, regulations, or government-wide policies.

b. PBGC's CUI SAO is PBGC's CUI Decontrol Authority and makes final determinations on decontrolling PBGC CUI upon an authorized holder's request.

c. Decontrolled CUI is still subject to PBGC's public release procedures.

d. Unauthorized disclosure of CUI does not constitute decontrol.

e. Authorized holders cannot decontrol CUI to conceal or avoid accountability for any unauthorized disclosure.

13. **CUI SELF-INSPECTION:**

a. PBGC's CUI Program conducts an annual self-inspection to measure and monitor implementation and management of PBGC's CUI program.

b. The self-inspection includes, among other elements, a method to resolve deficiencies and implement lessons learned.

14. **CUI MISUSE EVENT MANAGEMENT:**

a. All PBGC federal employees and contractors shall report CUI Misuse Events upon discovery using official reporting channels identified in PBGC's CUI Program Guidance documents.

b. The CUI Program conducts internal reviews of any CUI Misuse event impacting PBGC information and determines necessary mitigation strategies as appropriate. Such actions will focus on correcting or eliminating the conditions contributing to the CUI Misuse event.

15. **NON-COMPLIANCE:**

a. The discovery of non-compliance may occur during program compliance assessments, CUI Misuse event reports, or during the normal course of doing business. Covered individuals who do not comply with this policy, including the standards, procedures, processes, and guidance developed and disseminated by the CUI Program, may be subject to corrective, disciplinary and/or adverse action, as described in:

(1) PBGC Directive PM 30-01, for employees.

(2) PBGC Directive FM 15-03, for contractors.

b. A federal information system that does not comply with this policy, including the standards, procedures, processes, and guidance developed and disseminated by the CUI Program, is subject to CUI SAO review which may result in the CUI SAO recommending the system be barred from operating until the system is brought into compliance.

16. **TRAINING:**

a. Training is mandatory for all PBGC federal employees and contractors with access to or potential access to CUI. Initial CUI training is mandatory upon onboarding, and refresher training is required to be completed at least once every two years after that.

b. PBGC federal employees and contractors serving in certain roles (e.g., acquisition community) may also require supplemental mandatory training.