Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Customer Feedback Management System (CFMS) Privacy Impact Assessment (PIA)

Last Updated: 07/18/2025

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.6039
Email	diamante.catherine@pbgc.gov

2 PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) is 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 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.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as 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. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 13)*
Customer Feedback Management System (CFMS)	*CFMS is designed to measure customer satisfaction. The insights gathered support PBGC in enhancing service delivery and improving overall customer experience*	Yes	PBGC- 30	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. 301; 44 U.S.C. 3101 et seq.	No

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

The Customer Feedback Management System (CFMS) is a multi-tenant Software as a Service (SaaS) solution hosted on Amazon AWS GovCloud. Managed by the CFI Group, a FedRAMP-authorized provider, CFMS is designed to measure customer satisfaction. The insights gathered support for PBGC in enhancing service delivery and improving overall customer experience. Customers can complete surveys within the system, and their feedback is used to analyze and assess satisfaction levels.

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Low
Availability	Low

3. Is this a contractor system?

☒Yes
☐No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

CFMS is a new system

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

   (The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

No

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

PII is collected only if the survey respondent requests a callback/email from PBGC. The PII collected includes name, phone number for the callback or email address. The PII is necessary and relevant, because the survey is anonymous and without the customer providing the information, we would not be able to follow up when requested. There are not any procedures taken to review the accuracy, relevance, timeliness and completeness of the PII as it is used for a limited purpose and in a limited timeframe.

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

The identifiers include name, phone number and email address that the survey respondent provides if a callback/email is requested.

8. Approximately how many individuals' PII is maintained in the system?

A total of seven surveys are administered. Two surveys are administered annually, one survey is administered quarterly, and six surveys are administered daily. Annually, approximately 750 survey respondents request a callback from PBGC and in doing so, provides their name, phone number and/or email address.

9. Is the submission of PII by individuals voluntary or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

The submission of PII by individuals is voluntary. There is no outcome if an individual does not submit PII. Respondents only submit PII if they would like someone from PBGC to call them.

10. If your system collects Social Security Numbers:

    a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

N/A

    b. Under which authorized uses, as described in the "Reduction of use of Social Security Numbers (SSN) in PBGC" policy document?

N/A

c. If the answer to b., above is "Compelling Business Need," please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

N/A

11. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

The source from which PII is collected is from the individual. The format in which PII is collected is via phone or online. We do not solicit a survey respondent to provide PBGC with PII. The respondent only provides PII if they would like someone from PBGC to call/email them. Privacy Act Notice https://feedback.gov.cfigroup.com/PBGCPrivacy

12. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.) If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of that document.

Statement of Services is in place and below is the Privacy Clause for Inclusion in Interagency Agreement with DOI/CFI. Handling PBGC Data Clause with PII Addendum for Inclusion in IAA (July 2024) In the foregoing Interagency Agreement (IAA), the parties, their agents, employees, and contractors or subcontractors, are bound by Federal privacy law, including, but not limited to, the Privacy Act of 1974, 5. U.S.C. § 552a, as amended, and all binding government-wide regulations on the collection, maintenance, and use of agency data, including guidance from the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). In addition, the following standard Pension Benefit Guaranty Corporation (PBGC) protocols regarding information privacy will be followed, as appropriate: (a) To the extent that the work under this contract may give the U.S. Department of Interior's Federal Consulting Group (IBC), their employees, Contractors, and Subcontractors access to PBGC data, which includes, but is not limited to, controlled unclassified information (CUI), the IBC and/or Contractors or Subcontractors shall take

measures necessary to restrict access to and safeguard such data from unauthorized use and disclosure.

(b) Definitions:

(1) "Access" means the ability to retrieve, modify, copy, or move data from PBGC premises and IT systems as an authorized user.

(2) "Contractor" and "Subcontractor" shall include any officer, partner, employee, or agent of the IBC, their contractors or subcontractors, as applicable. The responsibilities and requirements imposed on the Contractor under this clause are equally applicable to any Subcontractors.

(3) "CUI" is 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 not 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.

(4) "Misuse of CUI" is the use of CUI in a manner not in accordance with the policy contained in Executive Order 13556 Controlled Unclassified Information; 32 CFR Part 2002; the CUI Registry; the policies, procedures, and guidance of PBGC's CUI Program; PBGC Directive IM 10-3, Protecting Sensitive Information; or the applicable laws, regulations, and Government-wide policies that govern the affected information. This includes intentional violations, unintentional errors in safeguarding or disseminating CUI, or designating or marking information as CUI when it does not qualify as CUI.

(5) "Record" means information created or received by PBGC employees and contractor employees that is evidence of PBGC's business activities and preserved, or appropriate for preservation, by PBGC. A record can be in any media format (e.g., paper, digital or photo) and should document business activities or decisions. Also, records are defined as either temporary (at some point in time they can be destroyed) or permanent (a record that should be permanently stored at NARA). Reference 44 U.S.C. 3301 for full definition.

(c) CUI Requirements

(1) When the contract requires the Contractor to access or maintain CUI, the Contractor and its Subcontractors must adhere to the requirements in Executive Order 13556, Controlled Unclassified Information; 32 C.F.R. Section 2002, Controlled Unclassified Information; the CUI Registry; the policies, procedures, and guidance of PBGC's CUI Program; and PBGC Directives IM 05-09, PBGC Privacy Program, IM 05-11, PBGC Insider Threat Program, IM 10-3, Protecting Personally Identifiable Information, and IM 15-03, PBGC Records Management Program.

(2) The Contractor agrees to maintain CUI in the strictest confidence. The Contractor also agrees not to publish, reproduce, or otherwise divulge CUI in whole or in part,

in any manner or form, nor to authorize or permit others to do so, taking such reasonable measures as are necessary to limit access to PBGC data to those Contractor employees needing such information to perform the work required under this contract. The IBC and Contractor also agree that CUI will only be released to those outside the PBGC after obtaining the required approvals as provided in PBGC's policies and procedures.

a. The Contracting Officer's Representative (COR) or point of contact for the IAA may require the IBC or Contractor to have any Contractor employees permitted access to PBGC data enter into a Non-Disclosure Agreement whereby the employee agrees not to discuss, divulge, or disclose any such information to any person or entity not directly concerned with performance of the contract work.

(3) CUI sent to a non-PBGC.gov address or shared with a non-PBGC employee shall be protected by encryption or transmitted within secure communication systems. Contractors and subcontractors shall not include any CUI in the subject or body of any email. Documents containing CUI shall be marked in accordance with PBGC's policies and procedures. Email attachments containing CUI shall be included as a password-protected attachment with the password provided under separate cover (i.e., separate email). Recipients of CUI shall comply with protections, restrictions, and limited dissemination controls imposed by the originator of the CUI.

(d) Cybersecurity Requirements

(1) The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by PBGC's Authorizing Official (AO). Once the ATO has been granted, the PBGC Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 1 year. An ATO is granted at the sole discretion of PBGC's AO and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(2) The Contractor shall adhere to PBGC Directive IM 05-02, PBGC's Information Security Policy; PBGC's Risk Management Framework; and NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations when conducting the annual Security and Privacy Assessment and Authorization (SPA&A) work.

(3) The PBGC may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The PBGC, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The IBC or Contractor shall afford PBGC, the Office of Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract.

Following a request from PBGC, the Contractor shall, through the Contracting Officer and COR, coordinate and participate in review and inspection activities by government organizations external to PBGC (e.g., GAO, CISA). Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Contractors operating information systems on behalf of PBGC shall comply with Federal reporting and information system continuous monitoring requirements. Annual, quarterly, and monthly data collection will be coordinated by PBGC. The Contractor shall provide PBGC with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with the requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, continuing monitoring of data must be maintained in accordance with PBGC's approved records management schedule.

(5) The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(e) Mandatory Training

(1) Prior to starting work on this contract, all Contractor employees assigned to work on this contract who receive a pbgc.gov email address shall be required to take any training required by PBGC to gain access to PBGC data or information systems. In addition, contractor employees working on this contract will be required to complete mandatory annual refresher training. Failure to complete this training by the required deadlines may result in the termination of the contractor employee's access to PBGC data until said training requirement is fulfilled.

(2) If the Contractor employees will not have a pbgc.gov email address, prior to starting work on this contract, the Contractor shall take Privacy and CUI training provided by PBGC and the COR shall maintain records of training completion. The Contractor employees working on this contract will be required to complete mandatory annual refresher training using the alternative training method. Failure to meet these requirements will result in PBGC requesting the Contractor employee be removed from working on the PBGC contract.

(3) All Contractors who have access to PBGC data are required to take annual refresher training.

(f) Reporting Incidents.

(1) The Contractor shall institute a process to ensure compliance with the provisions of this clause, and shall notify PBGC in writing, within 60 minutes of discovery, in the event that the Contractor determines or has reason to suspect an event that involves the actual or suspected Misuse of CUI or a cybersecurity event impacting the confidentiality, integrity, or availability of PBGC data.

(2) In such situations, the contractor shall notify the PBGC Service Desk by telephone (202-229-3999) and, thereafter, the contractor shall immediately email the PBGC Service Desk (desk.service@pbgc.gov) and CUI Program (CUIBreachReport@pbgc.gov), and also shall send a copy of the email message to the COR.

(3) The Contractor shall designate and identify an individual who will be responsible for the incident reporting and who shall be responsible to receive responses from PBGC and coordinate any further activity required by PBGC. Report of an incident by itself shall not be interpreted as evidence that the Contractor or Subcontractor failed to provide adequate safeguards for PBGC data.

(g) Incident Investigations. After initial report of the security incident or Misuse of CUI, the Contractor shall:

(1) Conduct a full investigation of the incident,

(2) Provide written updates regarding the investigation in accordance with a schedule set by the agency, and

(3) Provide a copy of the finalized incident/breach report as pertaining to PBGC data to the COR, Service Desk, and CUI Program Manager in writing prior to closing the incident/breach.

(h) Penalties.

(1) The Contractor may be requested to remove from any further contract work any employee who improperly discloses PBGC data. The CUI Program Manager (and Chief Privacy Officer for PII breaches), in connection with Security Operations, if necessary, shall document the reason for the removal request to the Contracting Officer. PBGC may terminate this contract for cause or default if the Contractor fails to comply with the provisions of this clause and also may exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

(2) If the Contractor or its Subcontractor misuse CUI, they are subject to penalties established in applicable laws, regulations and Government-wide policies including, but not limited to, 32 C.F.R. 2002.56, Sanctions for Misuse of CUI, and PBGC Directives IM 10-03, Protecting Personally Identifiable Information, IM 05-02, PBGC Information Security Policy, PBGC IM 05-11 Insider Threat Program, PBGC Information Security Policy, and FM15-03, Suspension and Debarment Program.

(3) Additionally, legal or criminal actions may also be initiated by the Office of Inspector General, the Department of Justice, and, when permitted, individuals harmed by the Contractor's action/inaction.

(i) The Contractor shall place the requirements contained in this clause in all subcontracts entered pursuant to the contract where the Subcontractor may have

access to PBGC data. The Contractor also agrees to be liable for any breach of the requirements of this clause by any and all Subcontractors under this contract.

(j) Privacy Requirements.

(1) Definitions

a. "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. Information that is not PII can become PII when it is combined with other information that is linked or linkable to an individual.

b. "Privacy Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized-user accesses or potentially accesses personally identifiable information or (2) an authorized-user accesses or potentially accesses personally identifiable information for an other-than-authorized purpose.

c. "Privacy Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint, voiceprint, or photograph.

d. "System of records on individuals" means a group of any Privacy Records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(2) When the contract requires the Contractor to design, develop, or operate a system of records on behalf of the agency, the Contractor is bound by section (m) of the Privacy Act, 5 U.S.C. 552a(m) and as such, is considered under the Privacy Act to be an employee of the PBGC. Accordingly, the Contractor is subject to the civil and criminal penalties of the Privacy Act, 5 U.S.C. 552a(i).

(3) If performance of the contract requires the design, development, or operation of a system of records on individuals, the Contractor shall comply with all Federal statutes, regulations, and guidance for such system of records, including, but not limited to, the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act, including guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology to accomplish an agency function when the contract specifically identifies:

a. The systems of records; and

b. The design, development, or operation work that the contractor is to perform.

(4) The contractor shall not remove PBGC data containing PII, whether in paper or electronic format, from approved locations or electronic storage without the prior written approval of the Chief Privacy Officer or their designees.

(5) Breach Reporting and Investigation.

a. When the Contractor or Subcontractor determines or suspects a Privacy Breach, they will report the breach within 60 minutes to the COR, Service Desk and CUI Program Manager as outlined as section (f) above, as well as to the Privacy Office at PrivacyBreachReporting@pbgc.gov.

b. In addition to sending a copy of the final investigation report as it pertains to PBGC data impacted by the incident, the Contractor shall send a copy of the report to the Chief Privacy Officer.

(6) Breach Remediation.

a. For PII breaches determined to be caused intentionally or by willful ignorance or not reported pursuant to the terms of this clause, the Contractor, in consultation with PBGC's Chief Privacy Officer, shall procure identity protection services equivalent to what PBGC would provide to any individual affected by a breach of PII if a federal employee were responsible.

(7) Penalties.

a. In addition to the penalties listed in section (h) above:
(i) In the event of violations of the Privacy Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Privacy Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

No, PII is not shared with external organizations.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	2	Phyllis Gaskins	Read, Write, add users, view any data coming in	2/5/2025

15. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

Physical Controls* - Physical security controls employed to secure the PII in the system include:

- Physical Access Authorizations
- Physical Access Control
- Access Control for Transmission Mission
- Access Control for Output Devices
- Monitoring Physical Access
- Visitor Control
- Access Records
- Power Equipment and Power Cabling
- Emergency Shutoff
- Emergency Power
- Emergency Lighting
- Fire Protection
- Temperature and Humidity Controls
- Delivery and Removal
- Alternate Work Site
- Location of information Components
- Information Leakage

*Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)

Technical Controls* - Technical controls employed to secure the PII in the system include:

- Account Management
- Access Enforcement
- Authenticator Management
- Cryptographic Module Authentication
- Information Flow Enforcement
- Separation of Duties
- Least Privilege
- Unsuccessful Login Attempts
- Remote Access
- Wireless Access
- Audit Events
- Audit Review, Analysis, and Reporting
- Time Stamps
- Audit Record Retention
- Non-repudiation
- Session Audit
- Public Key Infrastructure Certificates
- Denial of Service
- Network Disconnect
- Session Authenticity
- Protection of Information at Rest

**Technical Controls are provided by both PBGC

Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:

- Periodic Security Audits
- Regular Monitoring of User's Activities
- Annual Security, Privacy, and Records Management Refresher Training
- Backups Secured Offsite
- Encryption of Backups containing sensitive data
- Role-Based Training
- Least Privilege Access

Mandatory on-boarding training for security, privacy, and Records management personnel

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

We do not offer any additional training.

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

18. Does the system leverage the commonly offered control for Accounting of Disclosures?

☒ Yes
☐ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable retention schedule(s).

Records containing personally identifiable information (PII) are maintained and destroyed in accordance with the National Archives and Records Administration's (NARA) Basic Laws and Authorities (44 U.S.C. 3301, et seq.) and with PBGC-specific records disposition schedules approved by NARA. These retention schedules ensure that records are kept for the minimum period necessary to satisfy business, legal, and historical requirements. The following PBGC and General Records Schedules (GRS) govern retention and destruction of CFMS records:

GRS Items 6.5.010 and 6.5.020: Public Customer Service Records

grs06-5.pdf

2.3 Privacy Office Review

Name of Reviewer	Corey Garlick
Date Reviewed	7/18/2025
Expiration Date	7/18/2026
Result	☐☒ Approved without conditions ☐ Approved with conditions (see below). ☐ Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps).

Enter description here.

Discuss any conditions on Approval
