# Pension Benefit Guaranty Corporation

**Information Technology Infrastructure Operations Department (ITIOD)**

# Personnel Security Service (PSS)

# Privacy Impact Assessment (PIA)

Last Updated: 09/12/2025

# 1 PRIVACY POINT OF CONTACT

| Name | Catherine Diamante |
|------|--------------------|
| Title | Information System Security and Privacy Officer (ISSPO) |
| Phone | 202-403-4260 |
| 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 9)* |
|---|---|---|---|---|---|
| **eDelivery** | eDelivery is an electronic solution hosted by Defense Counterintelligence and Security Agency (DCSA). It provides PBGC's Information Technology Infrastructure Operations Department (ITIOD) with the ability to securely retrieve investigative files to process, adjudicate, and track the status of background investigation cases. | Yes | PBGC-12: Personnel Security Investigation Records | 29 U.S.C. 1302<br>5 U.S.C. 3301<br>44 U.S.C. 3101<br>EO 10577<br>EO 12968<br>EO 13467<br>EO 13488<br>5 CFR 5.2<br>5 CFR 731, 732 and 736<br>5 CFR 1400<br>OMB Circular A-130<br>FIPS 201<br>HSPD 12 | Yes |
| **USAccess** | The USAccess Program offers a shared service to PBGC with all the components necessary to manage the full lifecycle of a Personal Identity Verification (PIV) credential. This service allows for a single system to sponsor, enroll, issue, and maintain a common identity credential for each participant, and includes built-in workflow processes at every stage of the credentialing process. | Yes | PBGC-12: Personnel Security Investigation Records | 29 U.S.C. 1302<br>5 U.S.C. 3301<br>44 U.S.C. 3101<br>EO 10577<br>EO 12968<br>EO 13467<br>EO 13488<br>5 CFR 5.2<br>5 CFR 731, 732 and 736<br>5 CFR 1400<br>OMB Circular A-130<br>FIPS 201<br>HSPD 12 | Yes |
| **Personnel Security Investigation** | PSIS is a background investigation and security clearance request application. This application is a case management system that enables | Yes | PBGC- 12 - Personnel Security | 29 U.S.C. 1302<br>5 U.S.C. 3301<br>44 U.S.C. 3101<br>EO 10577 | Yes |

| 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 9)* |
|---|---|---|---|---|---|
| Solution (PSIS) | ITIOD to update and request relevant information about employees' and contractors' background investigations and security clearances. PSIS uses the separate eDelivery system to securely retrieve investigative files to process, adjudicate, and track the status of PBGC background investigation cases. | | Investigation Records | EO 12968 EO 13467 EO 13488 5 CFR 5.2 5 CFR 731, 732 and 736 5 CFR 1400 OMB Circular A-130 FIPS 201 HSPD 12 | |
| ServiceNow (SNow) GetITAccess New Employee Setup Form | After a new account creation request is submitted through GetITAccess, a Personnel Security Specialist uses this to create the PSIS' Intake Portal case.. | Yes | PBGC- 12 - Personnel Security Investigation Records | 29 U.S.C. 1302 5 U.S.C. 3301 44 U.S.C. 3101 EO 10577 EO 12968 EO 13467 EO 13488 5 CFR 5.2 5 CFR 731, 732, and 736 5 CFR 1400 OMB Circular A-130 FIPS 201 HSPD 12 | Yes |

## 2.2   The System as a Whole

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

> *PSS is a collection of solutions and processes supporting background investigations and security clearance case management. The system supports secure retrieval of investigative files to process, adjudicate, and track the status of background investigation cases and the resulting issuance of credentials. This subsystem is a FISMA child of the parent ITISGSS and is not FISMA reportable.*

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

    Confidentiality        Moderate
    Integrity              Moderate
    Availability           Moderate

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.

> *This is an existing information system. In May 2025, PBGC launched use of a new PBGC Applicant Intake Portal which allows applicants to securely submit required documents and information as part of the onboarding process directly to the Personnel Security Investigation Solution (PSIS) case management system. This streamlined approach reduces risk, enhances efficiency, and aligns with best practices.*
>
> *This replaced the combination of CORs receiving the PII via their email and uploading it to SharePoint.*

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.)

> *Individuals provide consent for the collection of this information as part of the background investigation, which is a requirement of employment.*

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 collected is used to perform background investigations to support the suitability and eligibility determination process for federal employees and contractors. PBGC Personnel Security limits PII collection only to what is needed to accomplish the stated purpose for its collection. Also, PII collected is necessary for production of the PIV card, in accordance with federal standards.*

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.

> *PSIS has multiple ways to query for an individual. The system takes the search filters and parameters (e.g. (first name, last name, Social Security Number, Date of birth etc.) identified by the user and sends a direct query into the database for specific base objects that match those filters. The database executes the query and returns the list of matching data objects.*

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

> Approximately 8000

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.

> Mandatory

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?

> *PII in the form of SSN is collected in support of background investigations and security clearance case management for PBGC employees and contractors.*

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

> ***Law enforcement, national security, credentialing****. Almost every law enforcement application must be able to report and track individuals using the SSN. This includes, but is not limited to, checks of the National Crime Information Center; state criminal histories; and FBI records checks.*
> ***Security clearance investigation or verification****. The conduct or verification of background investigations and security checks requires the use of the SSN. The SSN is the single identifier that links all aspects of these investigations together. This use is also linked to other Federal agencies that continue to use the SSN as the primary identifier.*
> ***Confirmation of employment eligibility.*** *Federal statute requires that all persons employed within the United States must provide an SSN or comparable identifier to prove that they are eligible to work for or with the government of the United States.*
> ***Oversight work conducted by the OIG****. Pursuant to the statutory authority of the OIG to act as an independent oversight unit of the PBGC programs and operations, OIG is not required to obtain Agency approval to conduct its oversight work in the form of criminal and administrative investigations, audits, inspections, evaluations, contract reviews, and other reviews. This oversight may require obtaining or using SSN to conduct criminal and administrative investigations, audits, inspections, evaluations, contract reviews, and other reviews.*

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.

> *Not Applicable*

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.

> *PII is collected from employees and contractors. The format for collecting PII includes forms submitted primarily via the PSS' Intake Portal. Email communication will be used as a secondary option in the event there are problems with the Intake Portal. Emails from PBGC would contain attached .pdf forms that are encrypted when being sent to new employees or contractors. PBGC advises new employees or contractors that any returned forms should be encrypted. The Intake Portal contains the PBGC's Privacy Act statement. The OF-306 and Fair Credit Reporting Act forms used are not PBGC forms and the Privacy Act Statements are the responsibility of the federal agencies that own these forms.*

> *All investigative case details, including PII, are retained in a secure IT system or safe with restricted access. Some information is pulled from other systems (General Services Administration (GSA) reports and Active Directory). Any DCSA mailed hard copy documents pertaining to PBGC applicant employee or contractor are scanned and uploaded into the PSIS application by PBGC Personnel Security unless the documents contain classified information, in which case, the hard copy documents are maintained in a PBGC safe as required by law.*

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.

> *PBGC does not inherit privacy controls from any external provider.*

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.

> *Currently, PSS leverages the eDelivery interface as outlined in the PBGC and DCSA ISA to securely retrieve investigative files. The ISA for eDelivery was signed on February 9, 2024, consists of three distinct aspects: the content, packaging, and delivery of investigative case material.*
>
> ***Content***
>     *The investigative content of the eDelivery investigative case material file.*
> ***Packaging***
>     *eDelivery packages the contents of an investigative file in a 256-bit encrypted ZIP file, the Distributed Investigative File (DIF). The DIF serves as an electronic representation of the investigative file and provides both a graphic representation of a printed file and a data representation of certain documents.*
> ***Delivery***
>     *PBGC investigative case material is received from DCSA via Secure File Transfer Protocol (SFTP) via a nightly batch transmission and transferred into PSIS manually by PBGC upon receipt. The transmission will include a crosswalk listing all cases included in the transfer and all corresponding DIF files.*
>
> ***USAccess****: Data collected by PBGC's enrollment station (Personnel Security) is transmitted to the USAccess Integrated Data Management System (IDMS) over an encrypted channel. Data is transferred to a GSA-contracted commercial smart card printing/personalizing provider over a Secure File Transfer Protocol (SFTP) connection. Data is also transferred to the Office of Personnel Management/DCSA over a Secure Virtual Private Network connection.*
>
> ***PSIS****: The Personnel Security Investigation Solution (PSIS) is built on Entellitrak Commercial Off the Shelf (COTS) application to enter and track information needed to support background investigations.*

*PII data is collected from PSIS to Symantec Data Loss Prevention (DLP) for Exact Data Matching (EDM). The data values are updated during the collection and only the numeric values are stored in DLP.*

*ServiceNow (SNow) GetITAccess New Employee Setup Form: To initiate the pre-screening process for new applicants, employees, or contractors, a New Employee setup form is submitted in GetITAccess. The PBGC's Personnel Security team creates a new Intake Portal case. The automated email workflow will send an email to the individual to fill out the OF-306 and Fair Credit Reporting Act form, along with uploading a copy of their resume.*

*National Background Investigation Services (NBIS): PBGC uses NBIS to initiate and submit eApps to initiate background investigations and re-investigations for PBGC employees. PBGC also requests copies of previous background investigations via NBIS. This data is shared with DCSA.*

14. For the user roles in the system:

| Role Name | Number of Users in that Role (AD) | Approver | Access Level (Read, Write, etc.) | Recertification Date |
|---|---|---|---|---|
| PSIS – Adjudicator | 4 | Manager/COR and PSS Administrator Business Owner | Create, Read, Update, Delete, Search | 7/24/2025 |
| PSIS – Admin Read Only | 3 | Manager/COR and PSS Administrator Business Owner | Read, Search | 7/24/2025 |
| PSIS – Administrator | 7 | Manager/COR and PSS Administrator Business Owner | Create, Read, Update, Delete, Assign, Search | 7/24/2025 |
| PSIS – Data Entry | 2 | Manager/COR and PSS Administrator Business Owner | Read, Update, Search | 7/24/2025 |
| PSIS - Supervisor | 2 | Manager/COR and PSS Administrator Business Owner | Create, Read, Update, Delete, Assign, Search | 7/24/2025 |
| PSIS – Security Specialist | 6 | Manager/COR and PSS Administrator Business Owner | Create, Read, Write, Update, Delete, Search | 7/24/2025 |

| PSIS – Adjudicator Low | 1 | Manager/COR and PSS Administrator Business Owner | Create, Read, Write, Update, Delete, Search | 7/16/2025 (New role created) |
|---|---|---|---|---|
| Intake Portal – Applicant User | N/A | Manager/COR and PSS Security Specialist | Read, Write, Update individual record (self) | N/A |
| Intake Portal – Administrator | 2 | Manager/COR and PSS Business Owner | Create, Read, Update, Delete, Assign, Search | 7/24/2025 |

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

*\*Physical Controls are provided by PBGC*

*Technical Controls\* - Technical controls employed to secure the PII in the system include:*
- o *Account Management*
- o *Access Enforcement*
- o *Authenticator Management*
- o *Cryptographic Module Authentication*
- o *Information Flow Enforcement*
- o *Separation of Duties*
- o *Least Privilege*
- o *Unsuccessful Login Attempts*
- o *Remote Access*
- o *Wireless Access*
- o *Audit Events*

- o *Audit Review, Analysis, and Reporting*
- o *Time Stamps*
- o *Audit Record Retention*
- o *Non-repudiation*
- o *Session Audit*
- o *Public Key Infrastructure Certificates*
- o *Denial of Service*
- o *Network Disconnect*
- o *Session Authenticity*
- o *Protection of Information at Rest*

***Technical Controls are provided by 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.

*Users of PSS must complete additional security training and training regarding the protection of PII offered by DoD.*

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).

---

*Security Management Records – Personnel Identification Credentials and Cards*: *Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use –* **GRS 5.6; Item 120**

*Security Management Records – Personnel suitability and eligibility investigative reports: Temporary. Destroy in accordance with the investigating agency instruction -* **GRS 5.6; Item 170**

*Security Management Records – Records of people not issued clearances:* *Temporary. Destroy 1 year after consideration of the candidate ends, but longer retention is authorized if required for business use -* **GRS 5.6; Item 180**

*Security Management Records – Records of people issued clearances: Temporary. Destroy 5 years after employee or contractor relationship ends, but longer retention is authorized if required for business use -* **GRS 5.6; Item 181**

*Security Management Records – Index to the personnel security case files:* *Temporary. Destroy when superseded or obsolete -* **GRS 5.6; Item 190**

*ITIOD:*

Per GRS5.6, investigative materials (saved in PSIS) are subject to the retention policies of the investigating agency, which is DCSA for PBGC. DCSA's retention period is 16 years for cases with no issues and 25 years for cases with issues. PSIS is not currently configured to comply with these schedules, and there are no manual processes in place. As a result, records are currently being held indefinitely.

---

## 2.3   Privacy Office Review

| | |
|---|---|
| **Name of Reviewer** | Margaret Drake |
| **Date Reviewed** | 9/15/25 |
| **Expiration Date** | 9/15/26 |
| **Result** | ☒  Approved without conditions<br><br>☐  Approved with conditions (see below).<br><br>☐  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

| |
|---|
| |