Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

ITISGSS Privacy Impact Assessment (PIA)

Last Updated: 08/26/2025

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.487.8102
Email	Hozey.lisa@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.

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.

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.

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)*
Microsoft Windows, UNIX, and LINUX Servers	Provides on premise server support for PBGC major information systems and applications.	Yes. For details on PII contained, review the PIA of the systems and applications supported by ITISGSS.	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28, 29)	The legal authority is identified under each PBGC major information systems/applications PIA, which is supported by the ITISGSS.	No.
Microsoft Structured Query Language (SQL) and Oracle Database Management Services	Provides on premise Microsoft SQL and Oracle database services support for PBGC major information systems and applications.	See first table entry.	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28, 29)	See first table entry.	No.
Veritas NetBackup and Azure Backup Systems	Provides information backup and recovery support for PBGC major information systems and applications.	See first table entry.	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27,28, 29)	See first table entry.	No.
Symantec Data Loss Prevention (DLP)	DLP solution being used to inspect all egress communications traffic, using content filters, to detect exfiltration of PII.	Yes.	PBGC-(**26**)	29 U.S.C. 1302(b)(3); 5 U.S.C. 301; 44 U.S.C. 3101; 44 U.S.C. 3554; Executive Orders 13587,13488,13467 and 3356	No.

2.2 The System as a Whole

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

*The **Information Technology Infrastructure Services General Support System** (ITISGSS) serves as a General Support System providing IT infrastructure support services to all PBGC major information systems/applications. Support services include Network Services, Internet Services, Telephony Services, Remote Access Services, Storage Services, Backup Services, File Transfer Services, File, Print and Fax Services, Development Tools, Release and Change Services, IT service management, Server Computing Services, End User Computing Services, Identity Credential and Access Management, Information System Security Services, and Shared Services. This is an existing system requiring an annual update and recertification.*

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 system and there are currently no changes.

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.)

The system does not collect, process or maintain any records that describe how an individual exercises First Amendment rights, but it does host applications that may do so. The information collected and it's purpose would be described in those applications PIAs.

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.

1) PBGC Connect Search Center
The PBGC Connect Search Center is used by PBGC employees, interns, and contractors to identify other PBGC employees, interns, and contractors; and, to access contact information for PBGC employees, interns, and contractors. Limiting collections of PII is controlled through two (2) means: (1) personal system data feeds only provide limited information and (2) providing limited fields for users to provide voluntary (i.e., not required of users and provided at their discretion) personal information.

2) Data Loss Prevention (DLP)
The PII ingested into DLP is restricted only to those fields being used for exact data matching and is used solely for the purpose of preventing the unauthorized exfiltration of the PII.

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 PII retrieved by the system is that contained in Microsoft Active Directory (AD) Services. Attributes on user objects under Microsoft Active Directory Services are populated and maintained through automated scripting against data feeds provided by the Procurement Department (PD) and the Human Resources Department (HRD). It is retrieved via the AD management tool Active Roles Server or the PBGC Connect Search Center. The identifiers are name and username.

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

Symantec DLP processes approximately 3-5 million records on individuals in the Symantec DLP tool - all PBGC employees and contractors, as well as pensioners and beneficiaries from Spectrum.

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.

It is voluntary, and the failure to submit the data would produce an outcome of not being able to use any of PBGC's applications or employee or contractor user services, since these services are only available via the use of an authorized AD username or application account.

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?

    The ITISGSS assumes a custodial role in protecting via DLP PII in the form of SSN transmitted and/or stored internally and through the incoming/outgoing of information by way of interconnections with external organizations.

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

    The GSS has a compelling business need to use SSNs. Specifically, ITISGSS uses SSNs collected by other systems to prevent the exfiltration of PII from PBGC's network using various data loss prevention tools.

    For the systems supported by ITISGSS, authorized uses of SSN can be found in the PIA of the specific subsystem or child PIAs.

    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.

    Because other systems must collect and use SSNs (see the relevant PIAs), the GSS cannot reduce its use of SSNs as they are used to protect the PII collected and maintained by PBGC.

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.

Sources from which the ITISGSS collects PII fall under two (2) areas:

1) *<u>PBGC Connect Search Center</u>*
   Sources of PII in the PBGC Connect Search Center include the PBGC employees, interns, and contractor staff and limited PBGC personnel records. PBGC Connect Search Center leverages Microsoft Active Directory Services to provide limited employee, intern, and contractor information.
   Attributes on user objects under Microsoft Active Directory Services are populated and maintained through automated scripting against data feeds provided by the Procurement Department (PD) and the Human Resources Department (HRD). Individuals are provided the ability to add additional personal information at their own discretion using the PBGC Connect Search Center interface. The PBGC Connect

Search information is only accessible to PBGC employees, interns, and contractor staff.

2) *Data Loss Protection (DLP)*

We have imported our data into the DLP solution as a protection mechanism to do exact pattern matching and prevent exfiltration from PBGC systems. PII data for our employees, contractors, and our pensioners (e.g., PSIS and BAS), as well as Controlled Unclassified Information (CUI) data from our financial systems (e.g., FMS), is ingested into the DLP solution for use in exact data matching.

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.

The ITISGSS contains twelve (15) subsystems and five (5) children. ITISGSS does not inherit privacy specific controls from external providers (e.g., Cloud Service Provider, third-party provider, another government agency, etc.). *Login.gov is the only Cloud Service Provider (CSP) currently offering privacy controls for inheritance*

For additional details regarding the externally inherited controls, see the Login.gov PIA.

The following ITISGSS ISA has privacy related sections, and they are summarized below:

CISA CLAW ISA:

- *Data Sensitivity*
  - *The data transferred from PBGC to the CISA is categorized as Federal Information Processing Systems (FIPS-199) "Moderate"*
- *Incident Reporting*

Each party will ensure that the other connecting party is notified when security or privacy incidents may have affected the confidentiality, integrity, or availability of the shared data or systems being accessed.

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.

The infrastructure elements of ITISGSS do not share PII, but the subsystems that are supported by the ITISGSS may. Internal sharing is identified under each PBGC major information systems or applications' PIA.

1) *PBGC Connect Search Center*
Personal data comes from automated Human Resources Department (HRD), Procurement Department (PD) data feeds, and through optional submission by individual users. The HRD and

PD data feeds populate Microsoft Active Directory user object attributes with select user object attributes presented under PBGC Connect Search Center.
PBGC Connect Search Center is used by PBGC employees, interns, and contractors to identify and access contact information of other PBGC employees, interns, and contractors.

2) <u>Data Loss Prevention (DLP)</u>
PBGC's DLP solutions are implemented to detect and prevent unauthorized exfiltration of PII outside the ITISGSS boundary. PII bound for the external network boundary but not authorized for release is either blocked or quarantined by the DLP solution. Metadata and, in some cases, limited extracts of the PII detected is stored in the local database used with the solution. Logs from the DLP are forwarded to the Security Information and Event Management (SIEM) solution but log data that is forwards does not contain PII.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Individual Users	2,291	Federal Managers/CORs spanning across the Corporation.	Access is role-based and is based on Access Control Lists (ACLs) needed to perform non-privileged duties as assigned.	June 20, 2025
Privileged Users	315	Federal Managers/ CORs spanning across the Corporation.	Access is role-based and is based on ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	June 20, 2025

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

- *Physical Controls - Entrance to PBGC HQ facilities employs armed guards and a PIV activated turnstile. Suites, to include the Network Operations Center (NOC), require a PIV for physical access. Physical security controls employed at PBGC HQ and colocation datacenters to secure the PII in the system include:*
  - *Security Guards*
  - *Secured Facility*
  - *Key Entry*
  - *Identification Badges (PIV)*
  - *Locked Offices*
  - *Locked File Cabinets*
- *Technical Controls - All PBGC users are required to go through the PBGC GetITAll Service Portal to request privileges to systems/applications. The granting of privileges is based on least privilege and separation of duties. Technical controls employed to secure the PII in the system include:*
  - *Password Protection*
  - *Virtual Private Network (VPN)*
  - *Firewalls*

- *Unique User Identification Names*
- *Encryption*
- *Intrusion Detection System (IDS)*
- *Personal Identity Verification (PIV) card access*
- *Public Key Infrastructure (PKI) Certificates*

- *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 and annual refresher training for security, privacy, and Records management personnel*

The above controls are also implemented for each cloud service but are shared between the Cloud Service Provider (CSP) and PBGC. Those controls provided by the CSP are implemented at the CSP's facilities. As indicated in question 4, for greater detail on subsystem controls, reference the subsystem PIA in question.

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

Additional training/guidance is provided by the PBGC Connect Governance Center, which hosts specific guidance on the acceptable use of PBGC technologies that may expose PII.

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).

A PBGC user's PII is retained in AD for the entire time the user is a PBGC employee, contractor or intern. Upon the termination of employment for the user, the deprovisioning process deletes the data, as per the PBGC Identity, Credential, and Access Management (ICAM) Standard.

Splunk logs for Data Loss Prevention (DLP) exact match data are retained for a total of six years: they remain readable for the first two years and are then archived for the remaining four years.

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	8/26/25
Expiration Date	8/26/26
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