Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

ITISGSS Privacy Impact Assessment (PIA)

Last Updated: 09/01/2022

1 PRIVACY POINT OF CONTACT

Name	Lester Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.3879
Email	hockman.lester@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.

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	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28)	The legal authority is identified under each PBGC major information systems/applications PIA, which is supported by the ITISGSS.	Internal sharing is identified under each PBGC major information systems/applications PIA, which is supported by the ITISGSS.
Microsoft SQL and Oracle Database Management Services	Provides on premise Microsoft SQL and Oracle database services support for PBGC major information systems and applications.	Yes	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28)	See first table entry.	See first table entry.
Backup and Recovery Systems	Provides information backup and recovery support for PBGC major information systems and applications.	Yes	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27,28)	See first table entry.	See first table entry.
Microsoft Office 365 Cloud Service: • **Advanced Threat Protection (ATP)**	ATP is a cloud-based email filtering service for cyber threat prevention and detection.	No		N/A	N/A
Microsoft Azure Government Cloud Service: • **Microsoft/*NIX Servers**	Provides cloud-based server support for PBGC major information systems and applications.	Yes	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28)	See first table entry.	See first table entry.
Symantec Data Loss Prevention (DLP)	DLP solution initially being used to inspect all egress communications traffic, using content filters, to detect exfiltration of PII.	Yes	PBGC-26, 27, 28)	See first table entry.	See first table entry.

2.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change).

*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.*

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

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. 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 four (4) areas:

1) *<u>PBGC Major Information Systems/Applications</u>*
   The primary source from which the ITISGSS collects PII is the PBGC major information systems/applications for which the ITISGSS supports. The ITISGSS assumes a custodial role in protecting information transmitted and/or stored internally and through the ingress/egress of information by way of interconnections with external organizations. Consult the PIA of the PBGC major information systems/applications for specifics on collection format and Privacy Act notifications given at time of PII collection.

2) *<u>Employee Retirement Income Security Act (ERISA) Filing Acceptance System (EFAST2)</u>*
   The ITISGSS maintains the EFAST2 Interconnection Security Agreement (ISA) with the Department of Labor (DOL). The EFAST2 ISA is for the sole purpose of obtaining data for consumption by other PBGC major information systems/applications. The EFAST2 ISA acknowledges the transfer of PII from EFAST2 and the general obligations to prevent unauthorized access or disclosure. Consult the PIA of the

PBGC major information systems/applications for specifics on collection format and Privacy Act notifications given at time of PII collection.

3) *PBGC Connect Search Center*
Sources of PII in the PBGC Connect Search Center include the subject individuals and limited PBGC personnel records. PBGC Connect Search Center leverages Microsoft Active Directory Services to provide limited employee, intern, and contractor information. Select attributes on user objects under Microsoft Active Directory Services are populated and maintained through mostly automated scripting against data feeds provided by the Procurement Department and the Human Resources Department. Individuals are provided the ability to add select additional personal information under their own accord using the PBGC Connect Search Center interface. The PBGC Connect Search information is only accessible to PBGC employees, interns, and contractor staff.

4) *Symantec Data Loss Protection*
Sources of PII in the DLP solution, from a collections perspective, are from subject individuals (within the ITISGSS boundary) attempting to enter their PII into an external system (external to the ITISGSS boundary) e.g., websites, banking, email, etcetera. Other PII is gathered, not deemed a collection, by subject individuals (within the ITISGSS boundary) attempting to send PII entrusted to the PBGC to an external entity (external to the ITISGSS boundary).

4. 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 seven subsystems and three children. The seven subsystems are cloud-based and include Microsoft Office 365 MT, Azure Government, ServiceNow, Everbridge Suite, Login.gov, Azure Commercial and Qualys Cloud Platform. O365MT, ServiceNow, Everbridge Suite, Login.gov and Qualys Cloud Platform hold FedRAMP authorizations at a moderate baseline; Azure Government and Azure Commercial have FedRAMP authorizations at a high baseline. PBGC does not inherit any privacy controls from the Cloud Service Providers (CSPs) for these subsystems, except for Login.gov. The three children of the parent ITISGSS include Physical Access Control and Surveillance System (PACSS), MyPBA/QuEST, Personnel Security System (PSS).

5. 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	10,396	Federal Managers/CORs spanning across the Corporation.	Access is role-based and is based in ACLs needed to perform non-privileged duties as assigned.	April 29, 2022
Privileged Users	1,863	Federal Managers/ CORs spanning across the Corporation.	Access is role-based and is based in ACLs needed to perform privileged duties as assigned. This includes network, system, & database administrators.	April 29, 2022

6. Does the System leverage the Enterprise Access Controls?

☒ Yes

☐ No

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

- *Physical Controls - Entrance to PBGC HQ facilities employ 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 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 GetIT 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 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 and PBGC. Those controls provided by the CSP are implemented at the CSP's facilities.

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

1) <u>PBGC Major Information Systems/Applications</u>
The specific uses, limits on PII collected, and necessity/relevance of PII, other than for storage in the ITISGSS, are identified under each PBGC information system's or major application's PIA supported by the ITISGSS.

2) <u>Employee Retirement Income Security Act (ERISA) Filing Acceptance System (EFAST2)</u>
The specific uses, limits on PII collected, and necessity/relevance of PII, other than for storage in the ITISGSS, are identified under each PBGC information system's or major application's PIA supported by the ITISGSS.

3) <u>PBGC Connect Search Center</u>
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 the 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 personal information.

4) <u>Symantec Data Loss Prevention</u>
PII collected, as well as gathered, by the DLP solution is solely for the purpose of preventing the unauthorized exfiltration of the PII.

9. 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.

1) *PBGC Major Information Systems/Applications*
The ITISGSS provides network infrastructure services for PBGC major information systems/applications. Network infrastructure services includes all the software and hardware configured to establish PBGC's Local Area Networks (LANs), Wide Area Network (WAN), and internet connectivity. Internal restrictions include a deny-all-allow-by-exception only rule for across environment server-to-server communications (production, development, and test). Consult the PIA of the PBGC information systems/major applications for specifics on data flows and applicable interconnections for those systems.

2) *Employee Retirement Income Security Act (ERISA) Filing Acceptance System (EFAST2)*
The ITISGSS provides network infrastructure services for PBGC information systems/major applications. Network infrastructure services includes all the software and hardware configured to establish PBGC's Local Area Networks (LANs), Wide Area Network (WAN), and internet connectivity. Internal restrictions include a deny-all-allow-by-exception only rule for across environment server-to-server communications (production, development, and test). The EFAST2 is a data source for PBGC information systems/applications. Consult the PIA of the PBGC information systems/major applications for consumption of, destinations out, and routine uses.

3) *PBGC Connect Search Center*
Personal data comes from automated Human Resources and Procurement Department data feeds. The data feeds are used to populate Microsoft Active Directory user object attributes with select user object attributes presented under PBGC Connect Search Center. Other PBGC Connect Search Center fields are optional and are left to an individual user to submit if desired. 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.

4) *Data Loss Prevention (DLP)*
Symantec's Data Loss Prevention (DLP) solution is being 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.

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

☒ Yes
□ No

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	10/6/22
Expiration Date	10/6/23
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

Enter description here.