Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Azure-Government Privacy Impact Assessment (PIA)

Last Updated: 09/17/2025

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-229-5607
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.

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)*
Platform as a Service (PaaS): APIM Compute Storage Networking Compute/Containers, Analytics Data Services Integration IoT Media/CDN Web/Mobile Power Platform	PaaS provides a managed hosting environment where PBGC systems can deploy applications without needing to manage Virtual Machines(VMs) or networking resources.	Yes	PBGC- (15, 16, 26)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 1302(b)(3); 44 U.S.C. 3554; 5 C.F.R. 731; 5 C.F.R. 302 OMB Circular A-130 EO 12656 EO 13587 EO 13488 EO 13467, as amended EO 13356	Yes
Infrastructure as a Service (IaaS): COTS Application PBGC Developed Application Database-Oracle & SQL Server Security Device Server-Windows Web Server-IIS Web Server-WebLogic	PBGC's responsibility is present at all service layers of Azure. PBGC is responsible for their applications hosted in Azure and for managing, for example, host-based firewalls, intrusion detection, and antivirus software.	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 EO 13587 EO 13488 EO 13467 EO 13356;5 C.F.R. 731; 5 C.F.R. 302 OMB Circular A-130	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)*
Sub-Components: App Gateway Databricks Data Factory DataLake	App Gateway, a web traffic load balancer, enables PBGC to manage traffic to web applications protecting PBGC applications from common web vulnerabilities. Databricks is a unified set of tools for building, deploying, sharing, and maintaining PBGC data. Data Factory is a cloud-based data integration service that allows PBGC to create data-driven workflow in the cloud for orchestrating and automating data movement and data transformation. DataLake integrates with other Azure services to provide a full data analysis solution.	No	N/A	N/A	No

2.2 The System as a Whole

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

***Microsoft Azure for Government (Azure-G)** is an open and flexible cloud platform that enables PBGC systems to quickly build, test, deploy, and manage applications, services, and product development across multiple datacenters located within the United States. PBGC business units can use Azure for building, deploying, and managing applications and services. Azure-G provides all layers of cloud offerings, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), and supports many different programming languages, tools, and frameworks, including Microsoft-specific, third-party, and open-source software and systems. Azure-G enables the building of large scalable applications serving large populations of users by scaling up or scaling down in short periods of time. The control baseline offered by Azure-G addresses a high security categorization per FIPS 199; however, since PBGC systems using Azure are categorized no higher than Moderate, only the security controls that are included in the NIST Moderate baseline are authorized by ITIOD for use.*

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.

Existing; no changes in its use.

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

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 the system does not collect, process or maintain records that describe how an individual exercises their First Amendment rights.

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.

The PII related to employees and contractors is used and needed to distinguish or trace an individuals' identity to authenticate users of the system. Limiting collection of PII is controlled through two means; (1) personal system data feeds only provide limited information and (2) providing limited fields for users to provide voluntary personal information. In order to comply with the provisions of the Privacy Act, Personally Identifiable Information (PII) captured will be secured in compliance with the Federal Information Security Modernization Act (FISMA) and not subject to unauthorized distribution.

Other PII in Azure-G is used by program offices within their system boundaries to perform the mission of the agency.

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 hosted on the system is specific to the applications hosted in Azure-G and the retrieval methods are specific to those applications.

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

PBGC administers the pensions of approximately 33 million+ individuals. Azure-G also contains the PII of approximately 8,000 employees and contractors.

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.

PII collected from employees and contractors for authentication purposes is mandatory.

PII collected from employees and contractors for background investigations is mandatory.

PII collected from employees, contractors, participant, or others is voluntary and the Privacy Act Statements for the systems that process the PII contains language outlining the consequences for failing to provide the requested PII.

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?

Not Applicable

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

Not Applicable

   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.

Azure-G indirectly collects PII via ITIOD applications (e.g., ARS and PSIS) and Oracle-based applications that have migrated to the Azure-G environment.

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.

Data flows are different for each application that is hosted in Azure-G. The PBGC User logs are based on the user subscription (subscription can be either web role based or worker role based). Based on the number of role instances specified by PBGC, Azure creates a persistent virtual machine (VM) for each role instance and then runs the role in the VM. The user then chooses from the several storage options provided. Sources of data that flows into the system includes all data associated with a wide range of applications and services- SQL server clusters, Windows servers, and Oracle database and servers.

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
Privileged Users	122	Federal Managers/CORs	Access is role-based and is based in Access Control Lists (ACLs) needed to perform duties as assigned	June 20, 2025
Individual Users	88	Federal Managers/CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 20, 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 (Information System Access)*

- *Access Control for Output Devices*
- *Access Control for Transmission Medium*
- *Monitoring Physical Access (Intrusion Alarms/Surveillance Equipment, Monitoring Physical Access to Information)*
- *Visitor Access Records (Automated Records Maintenance/Review)*
- *Emergency Lighting*
- *Emergency Shutoff*
- *Emergency Power*
- *Fire Protection*
- *Temperature and Humidity Control*
- *Water Damage Protection (Automation Support)*
- *Delivery and Removal*
- *Alternate Worksite*
- *Location of information System Components*

**Physical Controls are provided by Cloud Service Provider (CSP)*

- *Technical Controls** - Technical controls employed to secure the PII in the system include:*
  - *Password protection*
  - *Virtual Private Network (VPN)*
  - *Firewalls*
  - *Unique user identification names*
  - *Encryption*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Access Enforcement*
  - *Information Flow Enforcement*
  - *Separation of Duties*
  - *System Use Notification*
  - *Wireless Access Restrictions*
  - *Remote Access*
  - *Non-Repudiation*
  - *Time Stamps*
  - *Audit Record Retention and Generation*
  - *User Identification and Authentication*
  - *Device Identification and Authentication*

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

- *Administrative Controls** - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system are provided by PBGC and 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*

***Administrative Controls are provided by PBGC*

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

The training would be specific to the applications hosted on Azure-C that contain PII, not specific to Azure-G.

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).

System Access Records. Systems requiring special accountability for access:

Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. GRS: 3.2; Item 031

Azure-G hosts the applications that contain PII, and the processes used by those applications determine the means in which PII is retained or destructed.

2.3 Privacy Office Review

Name of Reviewer	Magaret Drake
Date Reviewed	9/17/25
Expiration Date	9/17/26
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
