Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Azure-G Privacy Impact Assessment (PIA)

Last Updated: 7/13/2023

1 PRIVACY POINT OF CONTACT

Name	Les 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)*
PaaS: APIM Compute Storage Networking Compute/Containers, AI 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 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 EO 3356	Yes
IaaS: COTS Application PBGC Developed Application Database-Oracle 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 3356;5 C.F.R. 731; 5 C.F.R. 302 OMB Circular A-130	Yes
Sub-Components: App Gateway Databricks Data Factory	App Gateway, a web traffic load balancer, enables PBGC to manage traffic to web applications protecting	No	N/A	N/A	No

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)*
DataLake	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.				

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).

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, 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. 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 not directly collected from PBGC employees and contractors in this system; rather it is accessed via Active Directory.

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.

No privacy controls are inherited from any external providers.

5. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
Individual Users	148	Federal Managers/CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 1, 2023

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* -Physical security controls employed to secure the PII in the system include:*
  - *Physical Access Control*
  - *Physical Access Authorization*
  - *Visitor Access Records*
  - *Delivery and Removal*
  - *Emergency Lighting*
  - *Fire Protection*
  - *Water Damage Protection*

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

- *Technical Controls** -. Technical controls employed to secure the PII in the system include:*
  - *Password protection*
  - *Remote Access*
  - *Wireless Access*
  - *Access control for mobile phones*
  - *Virtual Private Network (VPN)*
  - *Firewalls*
  - *Unique user identification names*
  - *Encryption*
  - *Intrusion Detection and Prevention Systems (IDPS)*
  - *Personal Identity Verification (PIV) card access*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Audit Events*
  - *Content of Audit Records*

- *Audit Storage Capacity*
- *Timestamps*

***Technical controls 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 include:*
  - *Periodic Security Audits*
  - *Regular Monitoring of User's Activities*
  - *Annual Security, Privacy, and Records Management Refresher Training*
  - *Role-Based Training*
  - *Least Privilege Access*
  - *Mandatory on-boarding training for security, privacy, and Records management personnel*

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.

The PII is used 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.

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.

The PBGC User logs in 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.

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

☒ Yes
☐ No

11. 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

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	9/6/23
Expiration Date	9/6/24
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.