Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Azure-Commercial Privacy Privacy Impact Assessment (PIA)

Last Updated: 09/16/2025

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.

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)*
***Microsoft Entra* B2C**	*Microsoft Entra* B2C, also known as B2C Customer and Partner Identity Management (CPIM), is an identity management service that enables customers to customize and control how customers sign up, sign in, and manage their profiles when using customer applications. This includes applications developed for iOS, Android, and .NET, among others. *Microsoft Entra (B2C)* enables these actions while protecting the identities of customers at the same time.	No	N/A	N/A	No
Microsoft Entra ID	Microsoft Entra ID is a cloud-based directory and identity management service. It combines core directory services, advanced identity governance and access management to deliver its services.	No	NA	NA	No
Dynamics 365	Dynamics 365 is Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) software package developed by Microsoft and offered via	Yes	PBGC- (6, 9, 19)	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 26 U.S.C.	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)*
	a FedRAMP-authorized cloud service. The Dynamics 365 Software as a Service (SaaS) model allows users to coordinate workflows and develop metrics for business operations within an organization.			6103; 44 U.S.C. 3101; 5 U.S.C. app. 105; 5 U.S.C. 301, 552(a), 552a(d), and 7101; 42 U.S.C. 2000e, et seq.; 44 U.S.C. 3101; 29 CFR 4003.1,4003	
InTune	InTune is a cloud-based service in the enterprise mobility management (EMM) space that helps enable a PBGC workforce to be productive while keeping corporate data protected. With InTune, it is possible to manage the mobile devices used by the workforce to access company data, manage the mobile apps utilized by the workforce, protect company information by helping to control the way the workforce accesses and shares it, and ensures devices and apps are compliant with company security requirements.	Yes	PBGC-(26)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 6120 1302(b)(3); 5 U.S.C. 301; 44 U.S.C. 3101; 44 U.S.C. 3554 EO 13587 EO 13488,13467 EO 3356 5 C.F.R. 731 5 C.F.R. 302 OMB Circular A-130	Yes
Power BI	Power BI is a suite of a collection of software services, apps, and connectors that work	No	N/A	N/A	N/A

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)*
	together to turn unrelated sources of data into sets of coherent, visually immersive, and interactive insights.				
Power BI Embedded	Power BI Embedded is a Microsoft cloud-based business intelligence solution that works from within Excel to analyze and visualize data.	No	N/A	N/A	N/A

2.2 The System as a Whole

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

***Microsoft Azure for Commercial (Azure-C)** is a public cloud platform that allows PBGC teams to efficiently build, test, deploy, and manage applications, services, and products across multiple U.S.-based data centers. Azure-C supports all cloud service models—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Currently, only SaaS components are in use, including Microsoft Entra ID, Microsoft Entra Business to Consumer (B2C), Dynamics 365, Intune, and the Power Platform (Power Pages, Power Automate, and Power BI).*

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 System, no changes since the last annual review.

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.)

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.

All PII collection/storage/usage is in line with the SORNs for the specific applications and PBGC policies, procedures and directives. None of the PII that PBGC has hosted in Azure-C is specific to Azure-C, it's all specific to the application or department hosted by/stored in Azure-C.

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.

This is all specific to the applications hosted within Azure-C and described within those applications' documentation.

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

PBGC administers the pensions of approximately two million individuals

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, the PII collected by the specific applications hosted in Azure-C is required to administer, manage legal cases (e.g. relating to individuals' pension plans, federal personnel action cases, etc.) and receive submissions from plan sponsors of ongoing plans

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?

PBGC uses the SSNs of participants in multi-employer plans that have applied for financial assistance to ensure that those listed in the plan census data have not been reported as deceased by Social Security prior to providing assistance based on the census data.

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

Government Data Matching. Systems, processes, or forms that interact with other government agencies or non-Federal databases may require the continued use of the SSN as a primary identifier as a primary means for transferring, matching, or checking information. These applications should be rigorously scrutinized to determine the availability of some other means of conducting these transactions.

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 indirectly collected from PBGC employees, contractors, plan sponsors and administrators, participants/beneficiaries, and vendors via Microsoft Entra ID. The format for collecting PII includes web interfaces such as MyPBA, eFiling Portal, and/or agency database. Individuals can opt out of this collection of PII as participants response on a PBGC form is voluntary. The eFiling Portal includes the Privacy Act Notice is located within the eFiling Portal.

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.

Any data sharing is specific to the applications hosted in Azure-C. Azure-C does not share data with external users.

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	25	Federal Managers /CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 20, 2025
Individual Users	2,291	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-C.

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

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