Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Azure-C Privacy Impact Assessment (PIA)

Last Updated: 08/26/2022

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)*
Azure Active Directory B2C	Azure Active Directory (AAD) B2C, also known as B2C 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. Azure AD B2C enables these actions while protecting the identities of customers at the same time.	Yes	PBGC- (6, 9)	29 U.S.C. 1055, 1056(d)(3), 1302, 1321, 1341, 1342, and 1350; 26 U.S.C. 6103; 44 U.S.C. 3101; 5 U.S.C. 301.; 29 CFR 4003.1,4003	Yes
Azure Active Directory (AAD)	AAD is a cloud-based directory and identity management service. Azure AD combines core directory services, advanced identity governance and access management to deliver its services.	Yes	PBGC-(6, 9)	29 U.S.C. 1055, 1056(d)(3), 1302, 1321, 1341, 1342, and 1350; 26 U.S.C. 6103; 44 U.S.C. 3101; 5 U.S.C. 301; 29 CFR 4003.1, 4003	Yes
Dynamics 365	Dynamics 365 is Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP) software package developed by Microsoft and offered via a FedRAMP-authorized	Yes	PBGC- (6, 9)	29 U.S.C. 1055, 1056(d)(3), 1302, 1321, 1341, 1342, and 1350; 26 U.S.C. 6103; 44 U.S.C. 3101; 5 U.S.C. 30129 CFR 4003.1, 4003	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)*
	cloud service. The Dynamics 365 Software as a Service (SaaS) model allows users to coordinate workflow and develop metrics for business operations within an organization.				
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 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 together to turn unrelated	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)*
	sources of data into sets of coherent, visually immersive and interactive insights.				
Power BI Embedded	Power BI 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, please include if this is an existing system (either an annual recertification update or a major change).

Microsoft Azure for Commercial (*Azure-C) is a public cloud platform that enables PBGC teams to quickly build, test, deploy, and manage applications, services, and product development across multiple datacenters within the United States. Azure-C provides all layers of cloud (IaaS, PaaS, and SaaS), however at this time only SaaS components are used; these include Azure Active Directory (AAD), AAD Business to Consumer (B2C), Dynamics 365, InTune, Power BI and Power BI Embedded.*

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 collected from PBGC employees and contractors, participants/beneficiaries, and vendors. The format for collecting PII includes web interfaces such as MyPBA and/or agency database. All data collection mediums include the PBGC Privacy & Paperwork Act Notices SHORT PRIVACY ACT NOTICE (pbgc.gov), Forms for Workers and Retirees | Pension Benefit Guaranty Corporation (pbgc.gov). *Individuals can opt out of this collection of PII as participant response on a PBGC form is voluntary.*

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	3,668	Federal Managers /CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 1, 2022
Participants/Public Users	84,468	Service Application Owner	Read/Write to own records	N/A

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 Authorizations*
  - *Physical Access Control*
  - *Access Control for Output Devices*
  - *Access Control for Transmission Medium*
  - *Monitoring Physical Access*
  - *Visitor Access Records*
  - *Emergency Lighting*
  - *Emergency Shutoff*
  - *Emergency Power*
  - *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 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*

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.

PII is used to authenticate and verify users of the system. For MyPBA, participants need to provide PII in order to use the system. PII is used to manage pension plan data; value pension plans and associated liabilities for which PBGC is, or may be, obligated to pay; calculate and provide pension benefits; and report tax information to the Internal Revenue Service (IRS) and other tax authorities. PII is also used to correctly identify pension plan participants enabling them to review pertinent information through the MyPBA web portal. 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 Management 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.

Azure Active Directory (B2C) *cloud service within Azure Commercial has been inserted between Azure and login.gov process as a middle layer. B2C receives authentication information from LG using the SAML protocol and then relays that information to MyPBA using Open Id Connect. When a user logs into the MyPBA portal using their credentials, a JSON web token is exchanged between MyPBA and Azure B2C where a custom policy transforms the JSON web token to SAML format. The SAML token is then exchanged between Azure B2C and login.gov to authenticate the user in login.gov. A JSON web token is sent back to MyPBA from Azure B2C to complete the authentication process.*

Azure Active Directory (AAD) *provides authentication and authorization assurances. The user presents credentials to AAD. AAD multifactor authentication works by requiring two or more authentication method, password, and username. AAD authenticates and redirects the user to an on prem server where the user is authenticated by using PIV cards.*

Dynamics 365 *relies on Azure Active Directory (AAD) to provide authentication and authorization assurance for all Dynamics 365 customer access and authentication attempts. Users at the Dynamics 365 portal are redirected to AAD to authenticate. Users after AAD authentication are redirected to ADFS server for authentication using their PIV cards. Data on PIV cards include Name, Social Security Number, Email Address, Telephone number, Date of Birth. AAD then validates the User and redirects back to the Dynamics 365 application where they are provided access to Dynamics resources associated with their user identity. (Dynamics 365 portal – AAD-ADFS-AAD – Dynamics 365)*

InTune*: InTune collects both personal and non-personal data from users. Personal data collected includes name and email address of PBGC mobile device users. Other non-personal data include device data/identifiers. Enrollment set up personal and non-personal data secures devices so that it aligns with PBGC's policies. Data ingested into InTune ensures the efficient management of PBGC mobile devices.*

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.