Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Office 365 (O365) Privacy Impact Assessment (PIA)

Last Updated: 09/21/2022

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)*
Exchange Online (EXO)	Provides cloud-based collaboration 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 authorities are reflected in each SORN as found on pbgc.gov/privacy.	Yes
SharePoint Online (SPO)	Provides cloud-based portal services for PBGC major information systems and applications. SharePoint Online includes Project Online and OneDrive for Business).	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 authorities are reflected in each SORN as found on PBGC.gov/privacy	Yes
MS Teams	Microsoft Teams (MSTeams) is an immersive workspace solution that provides instant messaging and group chat, voice/video calling and conferencing, file sharing, and shared workspace.	Yes	PBGC-(16)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301.	Yes
Information Protection (IP)	Provides anti-virus, anti-malware, and anti-spam filtering for email sent to Office 365. IP has built in message protections such as a message encryption, and other message protections in place to protect customer emails from unauthorized access and distribution.	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
Office Online	Provides the ability to view and edit, via web browser, documents in Office 365. Examples Include EXO attachments and SPO	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 authorities are reflected in each SORN as found on PBGC.gov/privacy	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)*
	documents. Office Online also includes the Office Collaboration Service (OCS) that allows users to collaborate in real-time on SPO-hosted documents no matter which client is being used (Desktop, Web, iPhone, Android).				
Delve	Allows users to manage their O365 profile, and to discover and organize the information that's likely to be most interesting across Office 365. Delve determines the relevancy of information based on the user's relationships as well as activity within the user's organization.	Yes	PBGC-(16)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301	Yes
Office Service Infrastructure (OSI)	OSI which is hosted on Azure provides a platform for backend applications that enhance the overall Office 365 service offering. PBGC Users do not interact with OSI.	No	N/A	N/A	N/A
Supporting Services	These include; Search Content Services (SCS), ORAS, AFS, Office Intelligent Services (IS), Cloud Input Intelligence (CII), LOKI, Bing, Customer Insight and Analysis (CIA), and O365 Suite User experience (SUE)	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).

Office365 *(O365) is a multi-tenant cloud computing-based subscription service offering from Microsoft. O365 provides PBGC with cloud versions of Exchange Online (EXO), SharePoint Online (Including Access Online and OneDrive for Business), Information Protection (IP), Office Online (WAC), Delve, and Microsoft Teams (MS Teams).*

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, contractors, students, and interns. PII from employees, contractors, participants and beneficiaries are captured from other data sources (eg; databases) and are transmitted into O365. Privacy Act Statements are the responsibility of the business office utilizing O365 to collect PII directly from an individual (e.g., using SharePoint of Office Forms)..

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

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:*
  - *Visitor Access Records*
  - *Physical Access Records*
  - *Emergency Shut off*
  - *Emergency Power*
  - *Emergency Lighting*
  - *Fire Protection*
  - *Temperature and humidity control*
  - *Water Drainage Protection*
  - *Delivery and Removal*
  - *Alternate Worksite*
  - *Location of information System Components*

**Physical Controls are provided by Cloud Service Provided (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*
  - *Intrusion Detection and Prevention Systems (IDPS)*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Remote Access*
  - *Wireless Access*
  - *Audit events*
  - *Audit Storage capacity*
  - *Time Stamps*
  - *Authentication Management*
  - *Identification and Authentication/Identifier Management*
  - *Cryptographic key establishment and Management*

***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.

O365 including its related components; Exchange Online (EXO), SharePoint Online, Information Protection (IP), Office Online, Microsoft Teams and Delve, collects maintains, uses, or disseminates: email addresses, names, contact information, SSNs, payment information, dates of birth, employment information, and other forms of PII of PBGC employees and contractors, participants and beneficiaries who communicate via O365 and its components. The limiting of PII collection is generally implemented at the collection point, which often is not O365; however, PBGC has taken steps to minimize PII in emails, eliminate it in Teams chats and file share, and ensure that documents with PII are saved only to those SharePoint sites marked as CUI.

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.

SharePoint Online (SPO) *uses multiple SQL databases (called content data bases), to store PBGC's data (Site content, list items, files, documents) on Azure encrypted storage. Sources of data include Files, documents, and site content. PBGC Users interact with SPO through web browsers. PBGC user authenticates to their own ADFS Infrastructure which will issue a ticket that AAD will validate; AAD then issues an internal ticket. SPO reads the ticket and based on the username and groups within, grants access to authorized SharePoint sites and files. PII on SharePoint may come from a number of data sources, including employees/contractors completing SharePoint forms, data extracts from databases, and the saving of documents containing PII on SharePoint.*
Exchange Online (EXO): *Email address, names, and phone numbers, are collected from individuals and stored in an "address book" data to provide full feature email capability for users. Exchange Online then creates a user ID, a unique email address created for the user to use when signing in to O365. The email address and a password created by the user authenticates and grants access to the user to receive and send emails. PII embedded in email addresses and PII attached to emails are also stored on EXO.*

MS Teams: *Users interact with MSTeams through MSTeams client and web-browsers. The user authenticates to their own Active Directory Federal Services (ADFS) infrastructure which will issue a ticket that Azure Active Directory (AAD) will validate. MSTeams reads the ticket and based on the permission grants access to authorized MSTeams resources. Calls, messages, voicemail, and IM conversations are stored in EXO/ Azure storage. While PII may be shared via screensharing in a meeting or call, PII should not be in a Teams chat or a file shared through Teams.*

Information Protection (IP): *The PBGC User authenticates to their own ADFS infrastructure which will issue a ticket that AAD validates; AAD the issues an internal ticket. IP reads the ticket and based on the username and group, grants access to view and modify the appropriate mail rules. PBGC emails are processed but not stored by IP. No IP PBGC content is sent outside of O365 other than to PBGC and PBGC interaction occurs over FIPS 140-2 compatible TLS. IP stores records flagged as violating the Microsoft DLP rules, which may include PII such as SSNs. These records are kept for 90 days and then deleted.*

Delve*: PBGC users interact with Delve via web browser protected by FIPS 140-2 compatible TLS. Users are then allowed to manage their O365 profile and to discover and organize relevant information across O365.*

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.