Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Office 365 (O365) Privacy Impact Assessment (PIA)

Last Updated: 9/17/2025

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)*
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, and 29)	29 U.S.C. 1302; 44 U.S.C. 3101; and 5 U.S.C. 301 ; 44 U.S.C. 301; 31 U.S.C. 6101; 31 U.S.C. 9101, et seq.; 31 U.S.C. 3716, 5 U.S.C. 5501-5584., 29 U.S.C. 1055, 1056(d)(3), 1302, 1321, 1341, 1342, and 1350; 26 U.S.C. 6103; 44, 5 U.S.C.7101; 42 U.S.C. 2000, 44 U.S.C. 3601, 5 U.S.C. 6120. 44 U.S.C. 3554, 29 U.S.C. 627, Executive Order 12977; 6 CFR part 37, 5 U.S.C. § 552, The Freedom of Information Act (FOIA)	Yes
SharePoint Online (SPO)	Provides cloud-based portal and content sharing services for PBGC major information systems and applications. SharePoint Online includes	Yes	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28, and 29)	Please see first row	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)*
	Project Online and OneDrive for Business.				
MS Teams	Microsoft Teams (MS Teams) 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
Purview Information Protection	Provides anti-virus, anti-malware, and anti-spam filtering for email sent to Office 365. Purview Information Protection 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 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).	Yes	PBGC-(1, 2, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 21, 22, 23, 25, 26, 27, 28, and 29)	Please see first row	Yes
Office Service Infrastructure (OSI)	OSI which is hosted on Azure provides a platform for backend	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)*
	applications that enhance the overall Office 365 service offering. PBGC Users do not interact with OSI.				
Supporting Services	Additional subcomponents support the Microsoft Office 365 environment. These include; Search Content Services (SCS), ORAS, AFS, Office Intelligent Services (IS), text prediction/autocomplete (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.

Office365 *(O365) is a subscription service offering from Microsoft to support business operations. O365 provides PBGC with cloud versions of Exchange Online (EXO), SharePoint Online (Including OneDrive for Business), Purview Information Protection, Office Online (Windows Admin Center (WAC)),,Microsoft Teams (MS Teams) and Supporting Services. PBGC uses O365 as 'evergreen' cloud-based services for email via Exchange Online, collaboration via Teams and SharePoint Online, document storage and sharing via OneDrive, the Office Suite (Word, Excel, PowerPoint, OneNote, Outlook, Publisher) Online and locally installed on PBGC users' laptops.*

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. Delve has been retired and its functionality has been integrated into other Microsoft 365 services, such as Microsoft Search and the Office 365 suite.

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.

O365 including its related components, Exchange Online (EXO), SharePoint Online, Purview Information Protection, Office Online and Microsoft Teams collects maintains, uses, or disseminates PII of PBGC employees and contractors, participants and beneficiaries, and vendors 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.

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 O365 is largely beneficiary, pension plan and participant documents stored on SharePoint Online and those documents are retrieved via secure browser or secure API integration with PBGC's business applications.

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

PBGC administers the pensions of approximately 33 million individuals. Additionally, there are currently 2141 PBGC 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.

It is voluntary, the PII collected by the specific applications and stored in O365 is required to administer those individuals' pension 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?

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.

PII is not collected directly from PBGC employees or contractors, but rather accessed or inherited through existing records—specifically, PII captured from Active Directory and transmitted into O365. Responsibility for providing Privacy Act Statements rests with the business units that use O365 tools (e.g., SharePoint or Office Forms) to collect PII directly from individuals.

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.

Exchange Online (EXO): *PII collected from individuals are stored in an "address book" data to provide full feature email capability for users. Exchange Online then creates 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.*

SharePoint Online (SPO) *uses multiple SQL databases (called content databases), 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 secure web browsers. PBGC users authenticate to PBGC's Active Directory Federation Services (ADFS) infrastructure which will issue a ticket that Microsoft Entra ID will validate; Microsoft Entra ID 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.*

MS Teams: *Users interact with MS Teams through MS Teams client and web-browsers. The user authenticates to PBGC's ADFS infrastructure which will issue a ticket that Microsoft Entra ID will validate. MS Teams reads the ticket and based on the permission grants access to authorized MS Teams resources. Calls, messages, voicemail, and Instant Messaging (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.*

Purview Information Protection: *The PBGC User authenticates to PBGC's ADFS infrastructure which will issue a ticket that Microsoft Entra ID validates; Microsoft Entra ID then 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 Internet Protocol (IP)Address. No IP PBGC content is sent outside of O365 other than to PBGC and PBGC interaction occurs over FIPS 140-2 compatible Transport Layer Security (TLS). IP stores records flagged as violating the Microsoft DLP rules, which may include PII collected. These records are kept for 90 days and then deleted.*

Office Online (Now known as Office for the Web):
The PBGC user access applications directly from their web browser without needing to install the desktop versions of the Office software. Office for the web is integrated with OneDrive, enabling easy collaboration and document sharing. Office for the web itself does not inherently store PII, but the documents created, edited, and stores within it may contain PII. These documents are stored on the SharePoint site.

MS Search/Office Suite: *Transport Layer Security (TLS) users are allowed to manage their O365 profile and to discover and organize relevant information across O365.*

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	67	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 2, 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.

No additional training other than the governance developed and published for PBGC's usage of O365 resources: https://pbgcgov.sharepoint.com/Sites/c-ConnectCafe/Governance/Articles/GovernanceHome.aspx

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).

Technology management administrative records: Temporary: *Destroy when 5 years old, but longer retention is authorized if needed for business use.* ***GRS 3.1; Item 001***

Infrastructure Project Records: Temporary: *Destroy when 5 years old, but longer retention is authorized if needed for business use****. GRS 3.1; Item 010***

System development records*: Temporary. Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.* ***GRS 3.1; Item 011***

Special purpose computer programs and applications: *Temporary: Delete when related master file or database has been deleted, but longer retention is authorized if required for business use.* ***GRS 3.1; Item 012***

Information technology operations and maintenance records: Temporary: *Destroy 3 years after agreement, control measures, procedures, projects, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.* ***GRS 3.1; Item 020***

Configuration and change management records: Temporary: *Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use.* ***GRS: 3.1; Item 030***

Information technology oversight and compliance records: Temporary: *Destroy 5 years after the project/activity/ transaction is completed or superseded, but longer retention is authorized if required for business use.* ***GRS:3.1; Item 040***

Documentation necessary for preservation of permanent electronic records: Permanent: *Transfer to National Archives with the permanent electronic records to which the documentation relates.* ***GRS: 3.1; Item 050***

All documentation for temporary electronic records and documentation not necessary for preservation of permanent records: Temporary: *Destroy 5 years after the project/activity/ transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.* ***GRS: 3.1;Item 051***

ITIOD: *Retention and destruction of PII data in O365 is governed by each department's Records Management Plan.*

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
