Template Version Number: 01-2021

U.S. Department of Commerce
U.S. Patent and Trademark Office

Privacy Impact Assessment
for the
M365 Internal

Reviewed by: Deborah Stephens, Bureau Chief Privacy Officer

▣ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

TIFFANY DANIEL Digitally signed by TIFFANY DANIEL
Date: 2025.12.19 07:24:32 -05'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
USPTO M365 Internal

Unique Project Identifier: EIPL-DS-14-00

Introduction: System Description

Provide a brief description of the information system.

The United States Patent and Trademark Office (USPTO) internal users require different Commercial off-the-shelf (COTS) productivity tools to communicate and collaborate with each other internally and external customers and stakeholders securely to achieve USPTO agency's mission. The Microsoft Office 365 (M365) Internal product of the Enterprise Infrastructure Product Line (EIPL) provides communication and collaboration tools and services using M365 Internal.

M365 Internal provides support and is responsible for the core infrastructure of M365 Internal including Exchange Online, SharePoint Online, OneDrive, Microsoft Teams, Office Services, and Bookings. Each Service Team is responsible for the configuration and feature settings within their perspective Service.

Address the following elements:

(a) Whether it is a general support system, major application, or other type of system

Communication and collaboration system

(b) System location

Government Community Cloud

(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

M365 Internal interconnects with:

Identity, Credential, and Access Management Identity as a Service (ICAM IDaaS) – is an Infrastructure information system, and provides authentication and authorization service to secure all enterprise applications/AIS's, provide audit ability to user activity. The system provides following services to the enterprise: User Provisioning and Life Cycle Management, User Roles and Entitlement Management, User Authentication and Authorization to protected resources, Application Integration/Protection, NIST controls compliance related to AU, AC, and IA family.

Private Branch Exchange-Voice Over Internet Protocol (PBX-VOIP) – is an infrastructure information system, consisting of the Cisco Voice Over Internet Protocol (VOIP), Enterprise Contact Center (ECC) and CRS that provides the following services in support of analog voice, digital voice, collaborative services and data communications for business units across the entire USPTO.

Enterprise Desktop Platform (EDP) –is an infrastructure information system, which provides a standard enterprise-wide environment that manages desktops and laptops running on the Windows 10 operating system (OS), providing United States Government Configuration Baseline (USGCB) compliant workstations. The USGCB security mandate by the Office of Management and Budget (OMB) requires all Federal Agencies, including the USPTO to use the directed desktop configuration.

Security and Compliance Services (SCS) – provides Security Incident and Event Management, Enterprise Forensic, Enterprise Management System, Security and Defense, Enterprise Scanner, Enterprise Cybersecurity Monitoring Operations, Performance Monitoring Tools, Dynamic Operational Support Plan, & Situational Awareness and Incident Response.

Patent Search System – Specialized Search and Retrieval (PSS-SS) – is Master system which supports the Patent Cost Center. It is considered a mission critical "system". PSS-SS provides access to highly specialized data that may include annual submissions of nucleic and amino acid sequence or prior-art searching of polynucleotide and polypeptide sequences, other types of information that may be more scientific or technology-based, Patent Linguistic Utility Service (a query by example search system), Chemical Drawing ability, and Foreign Patent Data.

Enterprise Software Services (ESS) – is comprised of multiple on-premise software services, which support the USPTO in carrying out their daily tasks. Within this system, the services are broken out into several subsystems. These subsystems are identified as AEM-OnPrem (AEM), DS-NiFi-API (NIFI), Enterprise Directory Services (EDS), Global Enterprise Architecture Repository System (GEARS), and USPTO Exchange Servers (PTOES).

(d) The way the system operates to achieve the purpose(s) identified in Section 4

M365 Internal is comprised of multiple cloud software services which support the USPTO in carrying out its daily tasks. Within this system, the services are broken up into several subsystems. Software subsystems include Email, OneDrive, Microsoft Teams, Bookings, and SharePoint.

Email

USPTO employees and contractors are able to access their personal M365 Internal Email via a web browser or the pre-installed application on their USPTO device. From there USPTO employees and contractors are able to view all messages that have been sent to them and send out Email communication to any valid Email address. Email communication allows the user to attach documents, send text, and invite individuals to meetings. Additionally, if someone is sending information that would constitute CUI, the user is able to label the email as CUI for external or internal communication. Additionally, the user is able to limit distribution and forwarding of the communication, encrypt and/or password protect the Email, if necessary.

OneDrive

USPTO employees and contractors can access OneDrive via a web browser or File explorer on their USPTO device. USPTO employees and contractors can save a variety of documents in OneDrive and are able to manage access to documents and/or folders the USPTO employee and contractor have created within OneDrive.

Microsoft Teams

USPTO employees and contractors are able to access their personal M365 Internal Microsoft Teams via a web browser or the pre-installed application on their USPTO device. Within the Microsoft Team application, the user can send messages to and have video and/or voice call with other USPTO employees and contractors with access to M365 Internal. Members of the public or employees/contractors of other federal agencies who receive a link to a Microsoft Teams meeting are able to join the video/audio call they have a link for. USPTO employees or contractors must admit the non-USPTO users for them to be able to be admitted to the call. That link provides the user access to that meetings chat and the call. During calls, USPTO employees and contractors are able to share their screen and can elevate access of external users to allow them to share their screen as well. Communication within Microsoft Teams can include attaching documents and images.

Bookings

USPTO employees and contractors can use the Bookings via the web application to assist with scheduling meetings. Bookings allows USPTO employees and contractors to list services they provide and the duration of time it will take to execute those services via a meeting. The individual wanting to schedule the service is able to select the service they want and Bookings will show the individual the available times they can schedule the service with the USPTO employee or contractor. USPTO employees and contractors who utilize Bookings can limit when these meetings can be scheduled, including when you are free, specific times/days, and require a lead time.

SharePoint
USPTO employees and contractors are able to access USPTOs M365 Internal SharePoint via a web browser on their USPTO device. SharePoint allows USPTO to provide information to USPTO employees and contractors to include webpages available to all USPTO employees and contractors, as well as sites with limited access. SharePoint sites can be updated by individuals with elevated access but users are set up by default as read only users.

(e) How information in the system is retrieved by the user

User access M365 Internal using multifactor authentication from desk client and web apps with their USPTO accounts. M365 Internal is using Okta cloud-based software as service solution to enforce multiple factor authentication.

(f) How information is transmitted to and from the system

Information is transmitted to and from M365 Internal via the internet and internal USPTO network. All communication is encrypted over TLS 1.2 higher using HTTPS protocols.

(g) Any information sharing

Internally, information can be pulled (automatically or manually) from M365 Internal and added to other internal system. M365 Internal includes USPTOs email communication and can be used to send information to non-USPTO email addresses. M365 Internal Microsoft Teams has a limited ability to share information with external users for the time users are accepted into a USPTO meeting.

(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information

The citation of the legal authority to collect PII and/or BII is 5 U.S.C 301, 15 U.S.C. 1051 et seq., 35 U.S.C. 2, and E.O.12862.

(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Moderate

<u>Section 1</u>: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

☒This is a new information system.

☐This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions	☐	d. Significant Merging	☐	g. New Interagency Uses	☐
b. Anonymous to Non-Anonymous	☐	e. New Public Access	☐	h. Internal Flow or Collection	☐
c. Significant System Management Changes	☐	f. Commercial Sources	☐	i. Alteration in Character of Data	☐
j. Other changes that create new privacy risks (specify):					

☐This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

☐This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	☐	f. Driver's License	☐	j. Financial Account	☐
b. Taxpayer ID	☐	g. Passport	☐	k. Financial Transaction	☐
c. Employer ID	☐	h. Alien Registration	☐	l. Vehicle Identifier	☐
d. Employee ID	☒	i. Credit Card	☐	m. Medical Record	☐
e. File/Case ID	☐				
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name	☒	h. Date of Birth	☐	o. Financial Information	☐
b. Maiden Name	☐	i. Place of Birth	☐	p. Medical Information	☐
c. Alias	☒	j. Home Address	☐	q. Military Service	☐
d. Gender	☐	k. Telephone Number	☒	r. Criminal Record	☐
e. Age	☐	l. Email Address	☒	s. Marital Status	☐
f. Race/Ethnicity	☐	m. Education	☐	t. Mother's Maiden Name	☐
g. Citizenship	☐	n. Religion	☐		

u. Other general personal data (specify):

Work-Related Data (WRD)					
a. Occupation	□	e. Work Email Address	☒	i. Business Associates	☒
b. Job Title	☒	f. Salary	□	j. Proprietary or Business Information	☒
c. Work Address	☒	g. Work History	□	k. Procurement/contracting records	☒
d. Work Telephone Number	☒	h. Employment Performance Ratings or other Performance Information	□		
l. Other work-related data (specify): Business Associates, Proprietary or Business information, and Procurement/contracting records are uploaded/stored/managed by user.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints	□	f. Scars, Marks, Tattoos	□	k. Signatures	□
b. Palm Prints	□	g. Hair Color	□	l. Vascular Scans	□
c. Voice/Audio Recording	□	h. Eye Color	□	m. DNA Sample or Profile	□
d. Video Recording	□	i. Height	□	n. Retina/Iris Scans	□
e. Photographs	□	j. Weight	□	o. Dental Profile	□
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID	☒	c. Date/Time of Access	☒	e. ID Files Accessed	☒
b. IP Address	☒	f. Queries Run	☒	f. Contents of Files	☒
g. Other system administration/audit data (specify):					

Other Information (specify)
M365 Internal may have any PII/BII via Microsoft teams, OneDrive, and/or Email.

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person	☒	Hard Copy: Mail/Fax	□	Online	☒
Telephone	☒	Email	☒		
Other (specify):					

Government Sources					
Within the Bureau	☒	Other DOC Bureaus	☒	Other Federal Agencies	□

State, Local, Tribal	□	Foreign	□		
Other (specify):					

Non-government Sources					
Public Organizations	□	Private Sector	□	Commercial Data Brokers	□
Third Party Website or Application			□		
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

The information in the systems accuracy is ensured by obtaining the information from M365 Internal. The users and system administrators are able to review and update their information in case of inaccuracy by putting in a help desk ticket to update M365 Internal. Additionally, PII/BII is transferred securely to M365 Internal.

The system is secured using appropriate administrative physical and technical safeguards in accordance with the National Institute of Standards and Technology (NIST) security controls (encryption, access control, and auditing). Mandatory IT awareness and role-based training is required for staff who have access to the system and address how to handle, retain, and dispose of data. All access has role-based restrictions and individuals with privileges have undergone vetting and suitability screening. The USPTO maintains an audit trail and performs random, periodic reviews (quarterly) to identify unauthorized access and changes as part of verifying the integrity of administrative account holder data and roles. Inactive accounts will be deactivated and roles will be deleted from the application.

2.4 Is the information covered by the Paperwork Reduction Act?

□	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
☒	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards	□	Biometrics	□
Caller-ID	□	Personal Identity Verification (PIV) Cards	□

Other (specify):

☒	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings	☐	Building entry readers	☐
Video surveillance	☐	Electronic purchase transactions	☐
Other (specify): Click or tap here to enter text.			

☒	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program	☐	For administering human resources programs	☐
For administrative matters	☒	To promote information sharing initiatives	☒
For litigation	☐	For criminal law enforcement activities	☐
For civil enforcement activities	☐	For intelligence activities	☐
To improve Federal services online	☐	For employee or customer satisfaction	☐
For web measurement and customization technologies (single-session)	☐	For web measurement and customization technologies (multi-session)	☐
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

All PII listed in section 2.1, except the proprietary business information is related to USPTO employees and contractors. This information is used for communication by USPTO employees and contractors internally and with external parties.

M365 Internal mainly has e-mail addresses for members of the public and employees of other federal agencies. However, M365 Internal may have any PII that may be sent or received via email as part of normal USPTO business.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

In the event of computer failure, insider threats, or attack against the system by adversarial or foreign entities, any potential PII data stored within the system could be exposed. To avoid a breach, the system has certain security controls in place to ensure the information is handled, retained, and disposed of appropriately. Access to individual's PII is controlled through the application, and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. These audit trails are based on application server out-of-the-box logging reports reviewed by the Information System Security Officer (ISSO) and System Auditor and any suspicious indicators such as browsing will be immediately investigated and appropriate action taken. Also, system users undergo annual mandatory training regarding appropriate handling of information.

NIST security controls are in place to ensure that information is handled, retained, and disposed of appropriately. For example, advanced encryption is used to secure the data both during transmission and while stored at rest. Access to individual's PII is controlled through the application and all personnel who access the data must first authenticate to the system at which time an audit trail is generated when the database is accessed. USPTO requires annual security role based training and annual mandatory security awareness procedure training for all employees. All offices of the USPTO adhere to the USPTO Records Management Office's Comprehensive Records Schedule that describes the types of USPTO records and their corresponding disposition authority or citation.

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	☐	☐	☒
DOC bureaus	☒	☒	☒
Federal agencies	☐	☐	☐
State, local, tribal gov't agencies	☐	☐	☐
Public	☐	☐	☐
Private sector	☐	☐	☐
Foreign governments	☐	☐	☐
Foreign entities	☐	☐	☐
Other (specify): if a user sends an Email to anyone the email address and Email content would be shared. External users who join/are added to a Microsoft Teams call would receive the information shared during that meeting which may include PII/BII.	☒	☐	☐

☐	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

☐	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☒	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
☐	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

☒	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage: ESS ICAM-IDaaS PBX-VOIP PSS-SS
☐	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public	□	Government Employees	☒
Contractors	☒		
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

□	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
☒	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: https://www.uspto.gov/privacy-policy	
☒	Yes, notice is provided by other means.	Specify how: This PIA service as notice.
□	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

☒	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Individuals have the option to add information within the application such as Mobile number, Home Phone number, Birthday, and Fax Number.
☒	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: Individuals do not have the opportunity to decline to provide their PII/BII, as it is necessary for the purpose for which it was collected.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

□	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
☒	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: Individuals do not have the opportunity to consent to particular uses of their PII/BII, as it is necessary for the purpose for which it was collected.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

☒	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Individuals have the ability to update some of the PII to include mobile number, home phone number, birthday, and fax number.
☒	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: No, individuals have the ability to submit a help desk request to adjust their PII/BII in ESS which would then overwrite the outdated or incorrect information in M365 Internal.

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

☒	All users signed a confidentiality agreement or non-disclosure agreement.
☒	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
☒	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
☒	Access to the PII/BII is restricted to authorized personnel only.
☒	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Audit Logs
☒	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): 12/1/2025 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
☒	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
☒	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 5 recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
☒	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
☒	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
☒	Contracts with customers establish DOC ownership rights over data including PII/BII.
☒	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
☐	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

PII within the system is secured using appropriate management, operational, and technical safeguards in accordance with NIST requirements. Such management controls include a review process to ensure that management controls are in place and documented in te System Security Privacy Plan (SSPP). The SSPP specifically addresses the management, operational, and technical controls that are in place and planned during the operation of the system. Operational safeguards include restricting access to PII/BII data to a small subset of users. All access has role-based restrictions and individuals with access privileges have undergone vetting and suitability screening. Data is maintained in areas accessible only to authorized personnel. The system maintains an audit trail and the appropriate personnel is alerted when there is suspicious activity. Data is encrypted in transit and at rest.

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

☒ Yes, the PII/BII is searchable by a personal identifier.

☐ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

☒	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: DEPT-25, Access Control and Identity Management
☐	Yes, a SORN has been submitted to the Department for approval on (date).
☐	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

General Records Schedules (GRS) | National Archives

☒	There is an approved record control schedule. Provide the name of the record control schedule: Information technology operations and maintenance records – GRS 3.1 (excluding 050) General Technology Management Records – GRS 3.1:012 – Special purpose computer programs and

	applications Information Systems Security Records – GRS 3.2 IT Development Project Records – GRS 3.1:010 System and Data Security Records – GRS 3.2:010
□	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
☒	Yes, retention is monitored for compliance to the schedule.
□	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding	□	Overwriting	□
Degaussing	□	Deleting	☒
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

□	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
□	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

☒	Identifiability	Provide explanation: Name, work location, phone number, email address and IP address can identify an individual.
☒	Quantity of PII	Provide explanation: A large amount of data items are collected and are limited to name, mailing address, telephone number (work, cell, or home), e-mail address and security questions for verification and authentication purposes.
☒	Data Field Sensitivity	Provide explanation: The data includes limited personal and

		work-related elements for identifying and authenticating users and does not include social security numbers of individuals
☒	Context of Use	Provide explanation: PII collection is part of administrative logging purposes and basic work contact information is shared by use of the address book in Exchange and Microsoft Teams.
☒	Obligation to Protect Confidentiality	Provide explanation: PII collection is part of administrative logging purposes and basic work contact information is shared by use of the address book in Exchange and Microsoft Teams.
☒	Access to and Location of PII	Provide explanation: Access is limited only to the identified and authenticated users and partners.
□	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

The PII in this system poses a risk if exposed. System users undergo annual mandatory training regarding appropriate handling of information. Physical access to servers is restricted to only a few authorized individuals. The servers storing the potential PII are located in a highly sensitive zone within the cloud and logical access is segregated with network firewalls and switches through an Access Control list that limits access to only a few approved and authorized accounts. USPTO monitors, in real-time, all activities and events within the servers storing the potential PII data and personnel review audit logs received on a regular bases and alert the appropriate personnel when inappropriate or unusual activity is identified.

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

□	Yes, the conduct of this PIA results in required business process changes. Explanation:
☒	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

□	Yes, the conduct of this PIA results in required technology changes. Explanation:
☒	No, the conduct of this PIA does not result in any required technology changes.