Version Number: 01-2017

U.S. Department of Commerce
International Trade Administration

Privacy Impact Assessment
for the
ITA Microsoft Office 365 Platform
(ITA_O365PF)

Reviewed by: Angenette Cash, 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

CATRINA PURVIS Digitally signed by CATRINA PURVIS
Date: 2020.09.21 17:14:04 -04'00' 09/21/2020

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

U.S. Department of Commerce Privacy Impact Assessment
ITA Microsoft Office 365

Unique Project Identifier: 2443

Introduction: System Description

Description of the information system and its purpose: *Provide a general description of the information system in a way that a non-technical person can understand.*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

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

The ITA Microsoft Office 365 (O365) platform is a general support system and major application.

b) *System location:*

The ITA O365 platform is a multi-tenant cloud computing-based subscription service offering from Microsoft residing entirely within Microsoft's enterprise cloud infrastructure. Cloud computing and has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. Further, as defined within NIST SP 800-145 (The NIST Definition of Cloud Computing), the service model for O365 is Software-as-a-Service (SaaS). SaaS is a model of software deployment whereby one or more applications and the computational resources to run them are provided for use on demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud subscriber does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings. ITA does not maintain, manage, or control the underlying O365 cloud infrastructure, which is housed and maintained by Microsoft entirely within CONUS.

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

The ITA O365 Platform connects with the ITA Active Directory (AD) authentication servers located in ITA's Amazon Web Services (AWS) US-EAST IaaS tenant and the ITA Microsoft Azure AD cloud service, as integrated into the ITA Network infrastructure for account management and authentication via Active Directory Federation Services (ADFS). There is no information sharing between the ITA O365 Platform and these cloud computing services. The ITA O365 Platform and component applications provide ITA personnel the platform to collaborate within the environment. These integrated applications share the same authentication process (ADFS) to provide the needed functionality for the operations of the cloud support

system. Resources located in these applications are restricted by default and permissions are granted based on least-privileged access.

d) The purpose that the system is designed to serve:

The ITA O365 platform provides collaborative cloud computing services within ITA. Microsoft O365 is a FedRAMP approved application using the Software as a Service delivery model. The applications contained in O365 include: Exchange Online (EXO), SharePoint Online (SPO) (including Office Online and OneDrive for Business), and Skype for Business (SFB). Data Loss Prevention (DLP) is also enabled in O365 through the compliance suite, providing capability to identify, monitor, and protect sensitive information within the platform. This protects sensitive information and prevents its inadvertent disclosure.

e) The way the system operates to achieve the purpose(s) identified:

Detailed descriptions of application tools offered in the O365 Platform are provided below:

Exchange Online (EXO) provides emailing services and calendar capabilities for ITA personnel. Data collected, maintained and disseminated in the email service may include: employee name, job title, office telephone number, user ID, photographs, date/time of access and task information. This information is shared internally within ITA. The ITA Global Address List (GAL) collects a portion of this information (employee name, job title, office telephone number) and shares it with the DOC GAL. Users interact with the application via web browser and software applications (for desktop and mobile devices).

SharePoint Online (SPO) enabled ITA personnel to share and collaborate with colleagues within ITA. Office Online and OneDrive for Business are enabled through this platform. Office Online enables browser-based viewing and editing of Microsoft Office documents. OneDrive for Business enables online storage and synchronization of documents. Data collected, maintained and disseminated in the SharePoint Online suite include: employee name, job title, office telephone number, photographs, date/time of access, project titles, and tasks for execution assigned to personnel. SharePoint provides enhanced security (especially in dealing with extremely large quantities of documents). Without the appropriately assigned permissions (controlled and managed via Active Directory), users cannot access documents or even know those documents exist. All data is locked down and accessible only to those with the official need to know. Users interact with the application via web browser and software applications (for desktop and mobile devices).

Offices within ITA (including Technology, Services, and Innovation) are currently in the process of migrating to SharePoint Online from ITA's legacy on-premises SharePoint system.

Skype for Business (SFB) offers ITA personnel instant messaging, audio/video calling, and online/broadcast meeting capabilities. Data collected, maintained and disseminated through SFB include employee name, job title, meeting information, photograph, date/time of chats and contact information such as office address, location, and telephone number. Meeting "free/busy" calendar information is shared with DOC for scheduling purposes. Users interact with the application via web browser and software applications (for desktop and mobile

devices). This service is slated for replacement in the coming two years with Microsoft Office 365 Teams.

The ITA O365 platform has a number of supporting services in addition to this core, customer-facing services. Each core and supporting service is supported by a unique group of developers, testers, and administrators referred to throughout this document as a "service team". Each service is deployed onto service-specific, Microsoft-managed cloud SaaS infrastructure. The services themselves may be configured by their respective service team, but the operation and maintenance of the cloud servers themselves is managed entirely by Microsoft. While each service team follows O365 policy, their services may have unique implementations of some security controls.

f) A general description of the type of information collected, maintained, use, or disseminated by the system:

This document is intended to cover internal uses of cloud-based services as employee collaboration tools. ITA employees using these collaboration tools provide the following information via Active Directory: first name, last name, work email address, username, work phone number, and office location. Generally, employees should not provide information beyond business contact information. Some tools (like Skype for Business) rely on Active Directory to pre-populate the user's account. In other cases, ITA personnel may send basic business contact information, such as first name, last name, and email address, to create an account.

Any programs or systems using collaboration tools that require information beyond basic business contact information will require their own privacy compliance documentation. Information maintained in DOC content management sites, such as SharePoint, will depend on the particular business processes for which the systems are established. Content management sites may be used to support DOC programs such as: human resources, financial management, acquisition services, etc. Therefore, systems may include a variety of information from or about the public. Program site managers are responsible for managing the content of their sites. Content management sites that contain PII, beyond business contact information, are governed by the SORN specific to the record types stored within the IT system and must be used in accordance with the purpose(s) enumerated in the SORN.

g) Identify individuals who have access to information on the system:

Only authorized ITA TSI personnel with privileged account credentials will have access to administrate the ITA O365 platform. Non-administrative information (e.g., ITA email) may be accessed only by users with valid, active ITA user accounts with the appropriate permissions to access it, controlled via ITA's Active Directory.

h) How information in the system is retrieved by the user:

Users access non-privileged information on the ITA O365 platform via HTTPS-encrypted

internet traffic routed through Microsoft's Cloud servers. Privileged access to O365 resources (including the Microsoft Exchange Control Panel and other administrative features) is only accessible to users with privileged credentialed accounts controlled via ITA's Active Directory. Users interact with the EXO, SPO, and SFB cloud service applications via web browser and software applications (for desktop and mobile devices).

i) How information is transmitted to and from the system:

Users access non-privileged information on the O365 platform via HTTPS-encrypted internet traffic routed through Microsoft's Cloud servers.

j) Any information sharing conducted by the system

The system provides internal sharing of information by way of email and external correspondence by using the email system. The ITA Global Address List (GAL) collects select user information (employee name, job title, office telephone number) and shares it with the DOC GAL.

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

Legal authority to collect PII and/or BII is contained in the following laws or Executive Orders as it may apply: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107; E.O. 131614; 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210-110; E.O. 12554; Public Law 100-71, July 11, 1987.

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

Moderate

The collaborative cloud computing systems within the O365 Platform boundary are compliant with the privacy control requirements and the associated documentation certified through the Federal Risk and Authorization Management Program (FedRAMP).

Section 1: 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): Acknowledgement of incidental collection of PII/BII in the system.					

X 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.

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

General Personal Data (GPD)					
a. Name	X	g. Date of Birth		m. Religion	
b. Maiden Name		h. Place of Birth		n. Financial Information	
c. Alias		i. Home Address		o. Medical Information	
d. Gender		j. Telephone Number		p. Military Service	
e. Age		k. Email Address		q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation	X	d. Telephone Number	X	g. Salary	
b. Job Title	X	e. Email Address	X	h. Work History	
c. Work Address	X	f. Business Associates			
i. Other work-related data (specify): Unknown collection is incidental.					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		d. Photographs	X	g. DNA Profiles	
b. Palm Prints		e. Scars, Marks, Tattoos		h. Retina/Iris Scans	
c. Voice Recording/Signatures		f. Vascular Scan		i. Dental Profile	
j. Other distinguishing features/biometrics (specify):					

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

Other Information (specify)

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	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): ITA's Global Address List (GAL) is exported to Department of Commence for inclusion into their online Global Address Book.					

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.

Technical Points of Contact must submit requests for new accounts.
Users sign a Privacy Act statement consenting to and acknowledging the accuracy of their PII as part of their employment.
Unused accounts are automatically disabled and/or removed on a schedule.

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.
X	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):			

x	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):			

x	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	X	To promote information sharing initiatives	X
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online	X	For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): To provide access to ITA network resources; any other potential PII collection is incidental/unintended.			

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).

The ITA O365 platform provides collaborative cloud computing services using the SaaS model. Its main purpose is to provide a platform for ITA personnel to collaborate and share work-related information, whether through their government-furnished workstations or mobile devices, in a more secure manner. The ITA O365 Platform collects PII solely for authentication purposes. Only PII necessary to authenticate the user's identity is collected by the system. ITA O365 is enabled for external sharing solely within the Department of Commerce for the purposes of contact information sync (i.e., a shared Global Address List between DoC agencies). The system is not designed or intended to collect, maintain, or disseminate PII for any other purpose, but this information may still be shared by users on the system individually and incidentally. Data Loss Prevention (DLP) tools embedded in the system identify, monitor and prevent inadvertent sensitive information from being shared unencrypted. This tool is used in the entire O365 suite.

5.2 Describe any potential threats to privacy 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.)

To reduce the risk of account compromise, ITA employs appropriate security controls for the system in accordance with NIST 800-53, as described in Section 8.1 below. Additionally, ITA mandates annual refresher Cyber Security Awareness Training (CSAT) to maintain access to their ITA user accounts. ITA user accounts that are not compliant with annual CSAT requirements are disabled. ITA user accounts are also automatically disabled after 45 days of inactivity. Disabled accounts are reviewed monthly and deleted after 45 days of disablement. ITA users also consent to a System Use Notification when accessing ITA systems. ITA O365 platform and its component applications are subject to continuous monitoring by system and security administrators. ITA also employs Data Loss Prevention (DLP) as described in section 5.2. Insider threats are also a potential threat to privacy for this system.

Section 6: Information Sharing and Access

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.)*

	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			X
DOC bureaus		X	
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): Preserved emails may be shared with other Federal agencies to respond to FOIA requests or to meet legal requirements	X		

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

- *The bulk transfer data is the ITA Global Address List (GAL) for inclusion in the DOC GAL.*

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

X	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: The ITA O365 Platform connects with the ITA Active Directory authentication servers located in ITA's Amazon Web Services (AWS) US-EAST IaaS tenant and the ITA Microsoft Azure AD cloud service, as integrated into the ITA Network infrastructure for account management and authentication. However, there is no information sharing between the ITA O365 Platform and these cloud computing services.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.2 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	X
Contractors	X		
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.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	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: ITA's Privacy policy & Privacy statements - https://legacy.trade.gov/privacy.asp: Department Digital Privacy Policy - https://www.osec.doc.gov/opog/privacy/digital_policy.html Commerce Privacy Policy - https://www.commerce.gov/about/policies/privacy Commerce Privacy Program – www.commerce.gov/privacy .	
X	Yes, notice is provided by other means.	Specify how: The following System Use Notification/Warning Banner is presented during authentication to all ITA IT systems: ********** ** WARNING!....WARNING!....WARNING! ********** **This is a United States Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.
	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:
X	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: This is an operational requirement by the Department of Commerce for all employees. Users accept the System Use Notification/Warning Banner whenever they authenticate into ITA IT systems.

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

X	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how: Users waive control over the uses of their PII upon signing their Privacy Act agreement upon the initiation of their employment. Employees and contractors sign a written Access and Use policy which specifies that data they choose to provide in DOC systems (including ITA) are non-private and could be used for investigation purposes as per CITR-022.

	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

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

X	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users are permitted to review and update their PII data (e.g., in the event of a name change) via a service request ticket submitted to the ITA TSI Service Desk. O365 includes a functionality where users may view/update their user profile and can request to withdraw PII submitted by them.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not: All PII collection is incidental.

Section 8: Administrative and Technological Controls

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

X	All users signed a confidentiality agreement or non-disclosure agreement.
X	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
X	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
X	Access to the PII/BII is restricted to authorized personnel only.
X	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: Only authorized government/contractor personnel are allowed access to PII within the system. Authorizations for users occur annually, at a minimum in accordance with applicable Bureau, Agency, and Federal policies/guidelines. In addition, audit logs are in place and assessed per NIST control AU-03, Content of Audit Records. Audit logs are kept via Splunk.
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 3/24/2020 ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
x	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J 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).
x	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
x	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish 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).*

Active Directory and other PII/BII sources are limited to privileged administrator access only. Non-credentialed users do not have access to these sources.
ITA IT systems employ a multitude of layered security controls to protect PII at rest, during processing, and in transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level, including (but not limited to) the following:

- Intrusion Detection / Prevention Systems (IDS/IPS)
- Firewalls
- Mandatory use of HTTPS for ITA public-facing websites
- Use of Trusted Internet Connection (TIC)
- Anti-virus software to protect host/end-user systems
- Encryption of databases
- HSPD-12 compliant PIV cards
- Access Controls

ITA IT systems also follow the NIST standards including special publications 800-53, 800-63, 800-37, etc. Any system within the ITA that contains, transmits, or processes PII has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The ITA also employs a Data Loss Prevention (DLP) solution embedded in the O365 platform, which provides deep content analysis that helps identify, monitor, and protect PI or BII in the system. DLP helps prevent exposure of PII, financial information, or intellectual property data sent via email. DLP is critical to the maintenance of privacy in enterprise message systems because business-critical email often includes sensitive data that needs to be protected and/or encrypted.

Section 9: Privacy Act

9.1 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."

X	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*: COMMERCE/DEPT-25 Access Control and Identity Management System http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html
	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.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: *NARA General Records Schedule 5.1*
	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:
X	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	X
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 as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

X	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 levels. *(Check all that apply.)*

X	Identifiability	Provide explanation: The data collected by the system is publically available data. The common signature lines of emails contain non-sensitive PII elements such as names of employee/contractor, office location, business telephone number and business email address.
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:

	Obligation to Protect Confidentiality	Provide explanation:
X	Access to and Location of PII	Provide explanation: Access to PII is only among authorized federal employees and contractors that might exchange such information via email.
	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.)

Active Directory and other PII/BII sources are limited to privileged administrator access only. Non-credentialed users do not have access to these sources. Only PII/BII necessary to authenticate the user's identity is collected by the system. As such, PII implicated is generally non-sensitive, such as employee/contractor first name, last name, work email address, username, work phone number, office location, and other basic business contact information as necessary. As such the risk to privacy for this system is low. The primary risks to the system are information misuse or compromised accounts, with mitigations discussed in section 5.2 above.

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:
X	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:
X	No, the conduct of this PIA does not result in any required technology changes.