Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OITS Cloud General Support System
(OITS CGSS)

Reviewed by: Wesley T. Fravel, 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
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=CATRINA PURVIS, 0.9.2342.19200300.100.1.1=13001002875743
Date: 2018.09.28 18:52:26 -04'00'

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

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary / OITS Cloud General Support System

Unique Project Identifier: OS071

Introduction: System Description

The Office of Information Technology Services Cloud General Support System (OITS CGSS) provides collaborative cloud computing services within DOC. OITS CGSS uses authentication servers physically contained in the Herbert C. Hoover Building (HCHB) and connected to the HCHB Network Infrastructure. Both Microsoft Office 365(MT O365) and IBM MaaS360 Mobile Device Management(MDM) referenced under this general support system are FedRAMP approved applications using the Software as a Service delivery model. The applications contained in O365 include: Exchange Online (EXO), SharePoint Online (SPO), 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.

MaaS360 integrates with O365 and improves the capability of the entire cloud offering. It provides OITS with the ability to manage and secure Department of Commerce (DOC) issued mobile devices such as smart phones and tablets, all from a centralized management solution. The applications process almost the same kind of data, though the functionalities differ.

This PIA is intended to cover internal uses of cloud-based services as employee collaboration tools. DOC 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, DOC 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.

SharePoint Online is currently being piloted in the Office of the Chief Information Officer organization. Upon successful pilot, the services may be expanded to other offices within the Office of the Secretary. Users interact with the application through web browser.

The following application tools are offered:

Exchange Online (EXO) provides e-mailing services and calendar capabilities for DOC personnel. Users interact with the application via software email clients and webmail

In compliance with Managing Government Records Directive (M-12-18), emails are preserved in content and structure, protected against their unauthorized loss or destruction, and remain discoverable, retrievable, and usable for the period specified in their retention schedule.[1] In implementing this directive, DOC has adopted the Capstone[2] approach to manage email records. The goal of this approach is to capture the email accounts of high level policy/decision makers and the accounts of those authorized to communicate on their behalf in the development of agency policy or important decision making. Given the value of these Federal records, the accounts of these individuals are kept permanently. The remaining records are held in accordance with the governing retention schedule.

- **Typical Data**: 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 tasks information. This information is shared internally and within other relevant Bureaus with the DOC.

SharePoint Online (SPO) enables DOC personnel to share and collaborate with colleagues within the Bureau and relevant DOC Bureaus. Access Online, Project Online, Delve and OneDrive for Business are enabled through this platform.

- Access is used to store information for reference, reporting and analysis.
- Project Online is used for planning and prioritizing projects.
- Delve enables viewing, editing and sharing documents.
- OneDrive provides online storage.

- **Typical Data**: Data that are collected, maintained and disseminated in the SharePoint 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 assigned permissions, users cannot access a document or even know the document exists. All data are locked down and accessible to only those with the official need to know.

Skype for Business Online (SFB) offers DOC personnel instant messaging, audio/video calling, and online/broadcast meetings capabilities. Users interact with the application through SFB client and web browsers.

---

[1] Criteria for Managing Email Records in Compliance with the Managing Government Records Directive (M-12-18), April 6, 2016, available at: www.archives.gov/files/records-mgmt/email-management/2016-email-mgmt-successcriteria.pdf.

[2] https://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html

• **Typical Data**: Data collected, maintained and disseminated through Skype include employee name, job title, meeting information, photograph, date/time of chats and contact information such as office address and location, telephone number by personnel within the Bureau and other relevant DOC Bureaus.

IBM MaaS360 Mobile Device Management(MDM) provides end-to-end management of mobile devices utilizing iOS and Android operating systems within the Bureau.

• **Typical Data:** MaaS360 contains data on security and compliance information such as password enforcement and apps control for the management of devices issued to DOC employees.

OITS CGSS connects with Office of Information Technology Services General Support System (OITS GSS-OSO64) authentication servers physically contained in the Herbert C. Hoover Building (HCHB) and connected to the HCHB Network Infrastructure. However, there's no information sharing between OITS GSS and the collaborative cloud computing services. The OITS CGSS provides DOC personnel the platform to collaborate within the environment. These integrated applications share the same authentication process 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 privilege access.

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); 5U.S.C. 5379; 5 CFR Part 537; DAO 202-957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999, DAO 210-110; Executive Order 12554, Public Law 100-71, dated July 11, 1987.

In accordance with Federal Information Processing Standards (FIPS) 199, the OITS CGSS has a system categorization level of **Moderate**. The collaborative cloud computing systems within the OITS CGSS system boundary are compliant with the privacy control requirements and the associated documentation are 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.
__X__ This is an existing information system in which changes do not 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):					

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):					
This PIA is intended to cover internal uses of cloud-based services as employee collaboration tools. Any programs or systems using collaboration tools that require information beyond basic business contact information will require their own privacy compliance documentation.					

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	X	p. Military Service	
e. Age		k. Email Address	X	q. Physical Characteristics	
f. Race/Ethnicity		l. Education		r. Mother's Maiden Name	
s. Other general personal data (specify): A user logs into the cloud system with his username and password, and the local Active Directory server located within the OITS GSS completes the authentication process.					

Work-Related Data (WRD)					
a. Occupation		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): The job title of a user does not provide any authentication to the system. It is only part of the user's email signature profile.					

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): Photographs are mainly profile pictures provided by the employee or contractor voluntarily.					

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address		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	X	Hard Copy: Mail/Fax		Online	X
Telephone	X	Email			
Other (specify):					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal		Foreign			
Other (specify): All DOC bureaus connect to the HCHBNet infrastructure.					

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 Contacts must submit requests for new accounts.
- Unused accounts are automatically disabled and/or removed on a schedule.
- Yearly account re-validation is conducted with all the Technical Points of Contact.

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): N/A			

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): N/A			

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

Section 4: Purpose of the System

The (OITS CGSS) provides collaborative cloud computing services using the Software as a Service (SaaS) model. Its main purpose is to provide a platform for DOC personnel to collaborate and share work-related information, whether through their work stations or mobile devices, in a more secured manner. Data Loss Prevention (DLP) embedded in the Office suite, identify, monitor and protect against the dissemination of PII or BII in the system. This tool is used in the entire MT O365 suite.

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		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify): Grant program requirements			

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 (OITS CGSS) provides collaborative cloud computing services using the Software as a Service (SaaS) model. Its main purpose is to provide a platform for DOC personnel to collaborate and share work-related information, whether through their work stations or mobile devices, in a more secured manner. The system can collect, maintain, disseminate PII shared by users individually. Data Loss Prevention(DLP) tool embedded in the systems identify, monitor and prevent inadvertent sensitive information which are unencrypted from being shared. This tool is used in the entire MT 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.)

There is a risk that a user's account could be compromised: To reduce the risk of account compromise, the DOC employees appropriate security controls for the system in accordance with NIST 800-53, as described in Section 8.1 below. Additionally, DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. Further, users sign an Access and Use policy (i.e. a "Rules of Behavior") for access to DOC systems. Finally, the OITS CGSS and applications on it are subject to regular monitoring by administrators.

There is a risk of inappropriate disclosure or use of data: DOC provides information security awareness training at the point of employee onboarding and mandates all end-user's complete refresher information security awareness training on an annual basis. This training focuses on threats that could lead to a compromised account, such as insider threats, phishing, and malicious attachments or hyperlinks. Further, users sign a Access and Use policy (i.e. a "Rules of Behavior") for access to and use of DOC systems and the information processed on them. Finally, the OITS CGSS and applications on it are subject to regular monitoring by administrators. As part of this monitoring, DOC has implemented a DLP program, as described below in Section 8.2.

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	X		
DOC bureaus	X		
Federal agencies	X		
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.

6.2 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: OITS CGSS OS071 connects with OITS GSS- OS064A's authentication servers physically contained in the Herbert C. Hoover Building (HCHB) and connected to the HCHB Network Infrastructure. No information is shared between any internal system within the network.
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 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

The Department of Commerce(DOC) Access and Use Policy published in CITR-022 provides for written acknowledgment of the Department or locally-derived policy by staff or contractors prior to gaining access to any public IT systems, networks or resources. Section 6.7 which is on privacy specifically reminds employees to be aware of the non-privacy of their information transmitted by or stored within the Agency's system.

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: https://connection.commerce.gov/policy/20140528/it-security-program-policy-commerce-informationtechnology-requirements-and-policy	
X	Yes, notice is provided by other means.	Specify how: Since users can choose to generate such information through emails, notice is provided via the user Access and Use Policy(CITR-022) and new hire training provided at the time of employment.
	No, notice is not provided.	Specify why not:

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

X	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how: Users generate and respond to emails voluntarily. Information that might be provided is specified through DOC policy(CITR-022). This does not apply to logon identification and password which authenticates users to the system.
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

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: Employees and contractors sign a written Access and Use policy which specifies that data that they choose to provide in DOC systems are non-private and could be used for investigations purposes as per CITR-022. This does not apply to logon identification and password which authenticates users to the system.
	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	Specify how: In case of PII generated through OITS CGSS and an

	them.	investigation necessitated, individuals may review/update information by Privacy Act Request.
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

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.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
X	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 7/14/2017 ☐ 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).
	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.
X	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).*

Data Loss Prevention (DLP) is embedded in the MT 0365, and provides deep content analysis that helps identify, monitor, and protect PII or BII in the system. DLP helps prevent exposure of PII, financial information, or intellectual property data sent via emails. 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.

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 provides coverage for the PII collected and maintained to facilitate secure on-line communication between Federal employees or contractors and to provide mechanisms for non-repudiation of personal identification and access to electronic systems. Content management sites, that contain PII beyond that covered by COMMERCE/DEPT-25, are governed by a 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.
	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: General Records Schedule 4.3 (130 (DAA-GRS-2013-0007-0012). with Transmittal No. 26, approved by NARA on September 2016.
	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 information contained in emails only identify a small number of system users that decide to expose such information
X	Quantity of PII	Provide explanation: OITS CGSS has 1400 users with a daily email volume of 28,000. The common signature lines of the emails contain non-sensitive PII elements such as names of employee or contractor, office location, business telephone number and business email address
X	Data Field Sensitivity	Provide explanation: The system contains contain non-sensitive PII elements such as names of employee or contractor, office location, business telephone number and business email address
	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 federal employees and contractors that might exchange such information through e-mail
	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.)

As outlined above, this PIA covers the cover internal uses of cloud-based services as employee collaboration tools. As such, PII implicated is generally non-sensitive, such as employee or contractor first name, last name, work email address, username, work phone number, office location, and other basic business contact information as necessary, or in some cases, photographs, voluntarily provided by employees as part of their user profile. As such, the risk to privacy for this system is low. The primary risks to the system are information misuse or compromised accounts as 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.