

**U.S. Department of Commerce
Office of Secretary**



**Privacy Threshold Analysis
for the
Office of Information Technology Services Cloud General Support
System (OITs CGSS)**

U.S. Department of Commerce Privacy Threshold Analysis

Office of the Secretary Cloud General Support System.

Unique Project Identifier: OSO71

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily predicated on the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy.

Description of the information system and its purpose: The Office of Information Technology Services Cloud General Support System (OITS CGSS) is a cloud computing-based subscription service with authentication servers contained in the Herbert C. Hoover Building (HCHB) and connected to the HCHB Network Infrastructure. Cloud versions of Exchange Online (EXO), SharePoint Online (SPO), Access Online, Project Online, Delve, OneDrive for Business, and Skype for Business (SFB) are all embedded in Microsoft Office 365 (MT 0365). EXO is an email service. SPO is a solution for creating sites to share documents and information. SFB is a communication service that offers instant messaging, audio/video calling, online/broadcast meetings and public switched telephone network services. There's however, a pilot program for the implementation of the SPO package in Office365 within the OITS CGSS environment. **MaaS360 Mobile Device Management (MDM)** is also integrated into the cloud General Support System. MaaS360 is a server and service that provides access to OITS users, and secure Department of Commerce data on mobile devices such as smart phones and tablets, all from a single screen. MaaS360 utilizes the Software as a Service(SaaS) delivery model, and its data contains no Personally Identifiable Information(PII). **Data loss prevention (DLP)** in Office 365 helps the Office of the Secretary identify, monitor, and protect sensitive information within the platform through deep content analysis.

The OITS CGSS platform provides federal staff and contractors, which are the primary users of the cloud email system the ability to create their own security and email distribution lists. MaaS360 enables customers to monitor and controls the security posture of their desktop and laptop devices. However, the EXO and SFB components of MT O365 has the potential to store Personally Identifiable Information (PII) provided users choose to exchange such data in the system. In accordance with Federal Information Processing Standard (FIPS) 199, the OITS CGSS has a system categorization level of **Moderate** due to the confidentiality of information pertaining to Executive and Congressional Liaisons functions.

Questionnaire:**1. What is the status of this information system?**

☐ This is a new information system. *Continue to answer questions and complete certification.*

☐ This is an existing information system with changes that create new privacy risks.
Complete chart below, continue to answer questions, and complete certification.

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	X
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	X
j. Other changes that create new privacy risks (specify):					

☒ This is an existing information system in which changes do not create new privacy risks. *Skip questions and complete certification.*

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

☐ . *Please describe the activities which may raise privacy concerns*

☒ No

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

☐ Yes, the IT system collects, maintains, or disseminates BII about: *(Check all that apply.)*

☐ Companies

____ ☐ Other business entities

__X__ ☐ No, this IT system does not collect any BII.

4. Personally Identifiable Information

4a. Does the IT system collect, maintain, or disseminate personally identifiable information (PII)?

As per OMB 07-16, Footnote 1: "The term 'personally identifiable information' refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc... alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc..."

__X__ Yes, the IT system collects, maintains, or disseminates PII about: (*Check all that apply.*)

__X__ ☐ DOC employees

__X__ ☐ Contractors working on behalf of DOC

____ ☐ Members of the public

____ ☐ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate PII other than user ID?

__X__ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4c. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

__X__ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, and/or 4c are “Yes,” a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the approved PIA must be a part of the IT system’s Assessment and Authorization Package.

CERTIFICATION


 X ☐ I certify the criteria implied by one or more of the questions above **apply** to the Office of Information Technology Services Cloud General Support System (OITS CGSS) and as a consequence of this applicability, I will perform and document a PIA for this IT system.

 ☐ I certify the criteria implied by the questions above **do not apply** to the Office of Information Technology Services Cloud General Support System (OITS CGSS) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Name of Information System Security Officer (ISSO) or System Owner (SO): Michelle Holland

Signature of ISSO or SO: Michelle Holland Digitally signed by Michelle Holland
DN: cn=Michelle Holland, o=Office of the Secretary, ou=Department of Commerce, email=Mholland@doc.gov, c=US
Date: 2016.12.14 12:23:01 -05'00' Date: 12/14/2016

Name of Information Technology Security Officer (ITSO): Jun Kim

Signature of ITSO:  Digitally signed by JUN KIM
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988
Date: 2016.12.13 13:44:39 -05'00' Date: 12/13/2016

Name of Authorizing Official (AO): Steven I Cooper

Signature of AO: RODNEY TURK Digitally signed by RODNEY TURK
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=RODNEY TURK, 0.9.2342.19200300.100.1.1=13001002898461
Date: 2017.01.13 16:07:11 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Michael Tolland

Signature of BCPO: MICHAEL TOLAND Digitally signed by MICHAEL TOLAND
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=MICHAEL TOLAND, 0.9.2342.19200300.100.1.1=13001000249566
Date: 2017.01.12 16:20:12 -05'00' Date: _____