Version Number: 01-2020

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
OS Cloud Services Platform
(OSCSP-OS071)

U.S. Department of Commerce Privacy Threshold Analysis
Office of the Secretary/Office of the Secretary Cloud Services Platform

Unique Project Identifier: OS-071

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 based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

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 Office of the Secretary Cloud Services Platform (OSCSP) 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 to include web spaces such as Connection.Commerce.gov. The overall system is comprised of FedRAMP authorized cloud services utilized to support enterprise-level end-user IT services to the Office of the Secretary and directly supported bureaus.

b) *System location*
OSCSP is comprised of several FedRAMP authorized cloud services. Implementation model is through a hybrid model whereby authentication is managed through both cloud and physical components residing within the Herbert Clark Hoover Building (HCHB). Physical system location of each cloud service within OSCSP is generally dependent on each vendor leveraging either Microsoft Azure or Amazon Web Services Infrastructure as a Service (IaaS)/Platform as a Service (PaaS).

c) *Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects.)*
OSCSP a Cloud General Support System with FedRAMP authorized cloud services. Authentication is provided through the Office of IT Services General Support System. Outside of these two systems, no other outside interconnections are permitted. Implementation model exists through a hybrid model whereby authentication is managed via both cloud and physical components residing within the Herbert Clark Hoover Building (HCHB), through which cloud services are accessed.

(d) The purpose that the system is designed to serve.

The OSCSP GSS provides enterprise-level IT service offerings to support end-users within the Office of the Secretary and supported bureaus. Services comprised under this system include the following:

Microsoft Azure is an open and flexible cloud platform (Infrastructure-as-a-Service) (IaaS) that enables customers to quickly build, test, deploy, and manage their applications, services, and product development across a network of Microsoft-managed datacenters within the United States. The Microsoft Azure Government platform exports savings to the customer by delivering the software, platform, and information technology infrastructure resources where and when it is needed via the Internet. The Microsoft Azure Government platform offers the same functionality in an environment dedicated to Government customers. The purpose is to increase the resiliency, dependability, and economy of providing IT services and functions by having them reside in the Microsoft cloud. The type of information collected, maintained, use, or disseminated are the End-user data files and application servers. OSCSP provides the platform for hosting Department of Commerce enterprise services and application.

Microsoft Office 365 Government Community Cloud (GCC) suite provides Exchange Online (EXO), SharePoint Online (SPO), Access Online, Project Online, OneNote, Delve, OneDrive for Business, and Teams 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. Teams is a unified communications platform that combines persistent workplace chat, video meetings, file storage and collaboration, and application integration.

ProofPoint is a Service-as-a-Solution (SaaS) employed by OESS to support compliance with Binding Operation Directive 18-01 for Domain-based Message Authentication, Reporting and Conformance (DMARC) and to provide additional security monitoring and enforcement controls for the O365 email services. Key capabilities include PFPT Protection Suite to include Targeted Attack Protection URL Defense & Attachment Defense, TAP Dashboard, Threat Response Auto-Pull, Dynamic Reputation, Spam, Virus Protection, Zero-Hour Anti-Virus, Email Firewall, Impostor email, graymail filtering, Smart, and Email Fraud Defense Suite.

Federal Computer Discovery Services (FCDS) (Relativity) The FCDS platform is a stand-alone system with no external interconnections. There are two main methods if file transfer/ ingestion, via Secure FTP (SFTP) and through physical delivery to CDS via encrypted hard drive. One or both methods may be used during the Relativity Pilot, depending on the needs of the Department of Commerce's (DOC or "the Department") Office of the Chief Information Officer (OCIO).

Granicus - GovDelivery Communications Cloud (GCC) is a standalone cloud-based system operated and managed by the Department of Commerce OS/ Office of Public Affairs (OPA) for providing available web content and mass email communications to the public. A public website is available for public subscription to web content and subscription emails. The service provides users with the ability to retrieve public subscriber information based on subject matter area so that web content and email messages can be crafted to specific public subscriber constituents. System users communicate with subscribers that opt into receiving communication on topics that matter to them. Information is transmitted to subscribers through System User crafted messages in Department of Commerce branded websites and email templates. Department of Commerce System Users can engage citizens with content by sending messages to a specific audience segment and save time by crafting a single message and sharing through the mass email service. ServiceNow Ticketing System (SNOW) is a SaaS service used to track all incidents and requests made to the OS/OCIO Service Desk. The Department of Commerce instances of ServiceNow are web-based and hosted in the FedRAMP high cloud by ServiceNow. The system is accessible to all Department of Commerce employees supported by the OS/OCIO Service Desk. The average user has limited access to make/view only their reported incidents and requests. Elevated access is granted explicitly by authorized personnel to service desk personnel and technical support staff to allows them to process incidents and requests. All users authenticate through ADFS Single Sign On or through the website. Information is retrieved exclusively through the website. ServiceNow retains basic information about employees including name, location and business contact information. ServiceNow syncs the user information from LDAP nightly by receiving an update. ServiceNow is not linked to any other systems and does not transmit any information.

Connection.Commerce.gov is the Department of Commerce intranet for DOC employees. This internal portal contains agency information on bureaus within the agency. The web space leverages cloud-based services to provide employees with collaboration information. DOC employees using these collaboration tools are supported through Active Directory authentication and generally do not use the tools to collect information beyond business contact information unless otherwise approved.

e) The way the system operates to achieve the purpose

The system leverages cloud-based services to provide employees with collaboration tools enhance productivity and enable high-performing computing capabilities. DOC employees using these collaboration tools are supported through Active Directory authentication and generally do not use the tools to collect information beyond business contact information unless otherwise approved.

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 online, 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.

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

The OSCSP system provides end-user computing capabilities to provide general file sharing capabilities and additional collaboration services through cloud services. The system in general is not used to collect information but serves as a repository for employees to store and share data. Additional services under the system provide documentation and tracking of IT service desk and change management requests. System purposes outside general end-user services have been documented in separate Privacy Impact Assessments.

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

The OSCSP provides access to all DOC personnel (federal employees and contractors) in the Office of the Secretary and supported bureaus to collaborate within the environment.

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

Information within the system is retrieved through role-based access control and active directory permissions through thick clients installed on the end-user's system and through web interfaces depending on the application.

i) How information is transmitted to and from the system

OSCSP 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.

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

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

__X__ 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	
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. *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

_____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

_____ Yes. This is a new information system.

_____ Yes. This is an existing information system for which an amended contract is needed.

_____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

__X__ No. This is not a new information system.

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.

__X__ Yes. *(Check all that apply.)*

Activities			
Audio recordings	X*	Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): **There is an option to use audio recordings through Microsoft Teams.*			

_____ 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.)."

__X__Yes, the IT system collects, maintains, or disseminates BII.

_____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual."

__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
_____ Other Federal Government personnel
__X__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 Social Security numbers (SSNs), including truncated form?

__X__Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form: There are varying needs for programs or systems using collaboration tools that require information beyond basic business contact information, which are supported by OSCSP. Those applications may require the need for SSNs, which will be provided in their accompanying privacy compliance documentation.

Provide the legal authority which permits the collection of SSNs, including truncated form. Section 3.04 of Department Organizational Order (DOO) 10-6 authorizes the Department's Office of General Counsel authority to "render all legal services necessary to enable the Secretary and the heads of operating units in the Department to discharge their respective duties"….and… "exercise direct or technical supervision over the provision of all legal advice and legal representation to the Department." Included in these duties is the need to collect information related to specific matters pertaining to the Department or to which the Department is a party. Information may include, as necessary, Social Security numbers, if, for example, the matter pertains to disbursement of funds to a current or former DOC employee. See also: 5 U.S.C. 301; 44 U.S.C. 31101; 42 U.S.C. 3211; 31 U.S.C. 240; 28 U.S.C. 533-535 and 1346(b); 15 U.S.C. 277 and 278e(b); E.O. 10450; E.O. 11478.

_____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. 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.

4d. 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, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP 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 OS Cloud Services Platform (OSCSP-OS071) 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 OS Cloud Services Platform (OSCSP-OS071) and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner
Name: Justin Strait
Office: OS/OIPS
Phone: 202-482-1128
Email: Jstrait@doc.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: JUSTIN STRAIT Digitally signed by JUSTIN STRAIT Date: 2021.09.14 07:58:04 -04'00'

Date signed:

Information Technology Security Officer

Name: Jerome Nash
Office: OS/OSSD
Phone: 202-482-5929
Email: JNash@doc.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: JEROME NASH Digitally signed by JEROME NASH Date: 2021.09.13 19:54:10 -04'00'

Date signed:

Privacy Act Officer
Name: Tahira Murphy
Office: OS/OPOG
Phone: 202.482.8075
Email: Tmurphy2@doc.gov

I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA.

Signature: TAHIRA MURPHY Digitally signed by TAHIRA MURPHY Date: 2021.09.14 10:57:57 -04'00'

Date signed:

Authorizing Official
Name: Lawrence W. Anderson
Office: Office of the Secretary
Phone: 202-482-2626
Email: LAnderson@doc.gov

I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system.

Signature: LAWRENCE ANDERSON Digitally signed by LAWRENCE ANDERSON Date: 2021.09.14 00:17:26 -04'00'

Date signed:

Bureau Chief Privacy Officer
Name: Maria D. Dumas
Office: OPOG
Phone: 202-482-5153
Email: MDumas@doc.gov

I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy.

Signature: MARIA STANTON-DUMAS Digitally signed by MARIA STANTON-DUMAS Date: 2021.09.14 11:57:07 -04'00'

Date signed: