Version Number: 01-2019

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
OS Cloud Services Platform
(OSCSP-OS071)

Reviewed by: Maria D. Dumas, 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

Jennifer Goode

08/12/2021

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

U.S. Department of Commerce Privacy Impact Assessment
Office of the Secretary/Office of the Secretary Cloud Services Platform

Unique Project Identifier: OS-071

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

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

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.

(e) 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.

(f) 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.

(g) Any information sharing conducted by the system

OSCSP is primarily accessed through the Herbert Clark Hoover Building (HCHBNet) and the Office of Information Technology Services General Support System (OITS GSS-OSO64) Information sharing is conducted within these two systems and collaborative cloud computing services within the OSCSP boundary.

(h) 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); 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.

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

In accordance with Federal Information Processing Standards (FIPS) 199, the OSCSP has a system categorization level of **Moderate**. The collaborative cloud computing systems within the OSCSP system boundary are compliant with the privacy control requirements and the

associated documentations 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.

__X__ 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	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.

____ 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).

____ 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 01-2017 or later).

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

Additionally, the PIA covers additional uses of the system for the Office of the General Counsel:
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, as amended and all other authorities of the Department.

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

u. Other general personal data (specify):

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 other data, such as criminal history if, such information is relevant to a matter or proceeding.

Work-Related Data (WRD)					
a. Occupation	X	e. Work Email Address	X	i. Business Associates	
b. Job Title	X	f. Salary	X	j. Proprietary or Business Information	X
c. Work Address	X	g. Work History	X		
d. Work Telephone Number	X	h. Employment Performance Ratings or other Performance Information			

k. Other work-related data (specify):

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	X	f. Vascular Scan		i. Dental Profile	

j. Other distinguishing features/biometrics (specify):

* Photographs are provided voluntarily, per the O365 identification settings for user profiles. They can be removed at any time by the user.

System Administration/Audit Data (SAAD)					
a. User ID	X	c. Date/Time of Access	X	e. ID Files Accessed	X
b. IP Address	X	d. Queries Run	X	f. Contents of Files	X
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	X	Online	
Telephone	X	Email	X		
Other (specify): **The system stores and manages documents which may include PII collected directly from individuals to whom the information pertains at the original point of collection or creation of a document. The system itself does not directly request or collect PII from individuals.*					

Government Sources					
Within the Bureau	X	Other DOC Bureaus	X	Other Federal Agencies	X
State, Local, Tribal	X	Foreign	X		
Other (specify): **The system stores and manages documents which may include PII collected directly from Government sources at the original point of collection or creation of a document. The system itself does not directly request or collect PII.*					

Non-government Sources					
Public Organizations	X	Private Sector	X	Commercial Data Brokers	
Third Party Website or Application					
Other (specify): **The system stores and manages documents which may include PII collected directly from Non-government sources at the original point of collection or creation of a document. The system itself does not directly request or collect PII.*					

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

The system will only be used as a medium to store and manage documents and associated data and files in a centralized location. The OSCSP system does not and will not verify the accuracy of the files maintained in the system or the contents therein. Information is verified for accuracy and currency at the time of collection, creation, or by mechanisms specific to source system from which it is derived. Data within documents in the OSCSP is obtained from DOC bureaus, offices and agency officials and is not verified for accuracy by the OSCSP system. The originating DOC bureau or office providing the information for each database is responsible for ensuring the accuracy of information included in the OSCSP. That said, the OSCSP provides Audit logging, which can help ensure that the information provided in the system is only accessed by authorized DOC users with appropriate permissions, reducing the risk of information being changed or modified, or otherwise compromising the integrity of information in the system.

2.4 Is the information covered by the Paperwork Reduction Act?

X	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection. Commerce Connect COVID Vaccine Attestation Survey is used for collecting medical information and resolution of HR-related requirements to validate DOC Federal Employees vaccination status. Commerce Connect (and OMB control numbers) are specific to the form being used to collect source information at the original point of collection.
	No, the information is not covered by the Paperwork Reduction Act.

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

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

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

	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	X	For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

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

The OSCSP 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 workstations 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 Office 365 suite.

Additionally, PII and BII maintained and processed by the system is used in the execution of the DOC OGC's Employment, Litigation, and Information (ELI) mission. The information is required for several reasons including, but not limited to:

- Confirming and identifying appropriate personnel, offices, and parties in legal actions and matters;
- Ensuring the proper disbursement of funds in employment, tort, property, and other matters involving a disbursement of funds; and
- In the review and analysis of commercial law matters.

The PII and BII identified in Section 2.1 can pertain to federal employees, contractors, and other staff, member of the public, foreign nationals, visitors, or any other party involved in a legal matter with the Department.
It is important to note that the system itself does not make determinations about individuals, however, the information in the system is used to process case files, and the disposition of a case could involve a determination about an individual.

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit

has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

There are several risks to personal privacy posed by DOC's use of the OSCSP: There is a risk of insider threat, or inappropriate use and protection of information in the OSCSP. There is a risk that PII or BII, including sensitive PII, could be misused, lost, or otherwise compromised. DOC has implemented controls which limit access to and use of the system to those employees with a clearly defined need-to-know the information. Additionally, the system has an auditing capability that tracks access to each document in the system, including which user accessed the document and when (date and time). There is a risk that aggregation and "connection" of multiple documents using metadata, as well as the enhanced search capabilities will create new information about individuals. As information in the system is derived from existing information or documents within and across DOC systems, the centralizing of such information for case and document management poses little risk to individual's privacy. Similar capabilities already exist within the systems that house such information. There is a risk that the system may collect or process unnecessary PII. There may be unnecessary use and sharing of PII if Data Loss Prevention (DLP) is not in place. Also, DLP may be present on some instances, but may not always prevent the loss of PII. Documents in the system are subject to legal and regulatory requirements, requiring that complete document collections be maintained, including documents that contain PII. All DOC personnel are also required to take annual cybersecurity and privacy awareness training. System administrators are also required to sign rules of behavior.

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		X
DOC bureaus	X		X
Federal agencies	X		
State, local, tribal gov't agencies	X		
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: The OSCSP connects with the Office of Information Technology Services General Support System (GSS) (OS-064). The OS-064 provides basic end-user access and authentication controls for the OSCSP. In addition to Microsoft provided controls, OSCSP inherits certain security functions and capabilities from the OITS GSS as well as HCHBNet. Additional information about the controls in place for OS-064 are available in the system's PIA.
	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

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.	
	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: _____.	
X	Yes, notice is provided by other means.	Specify how: The OSCSP does not directly collect information, rather, it serves as document repository for documents and materials which may be generated from source materials collected directly from individuals. As such, notice may be provided directly to impacted individuals at the time of collection, via form or other methods. Forms implicated include, but are not limited to: Standard Form 95 (SF-95) FMS 194: Judgement Fund Transmittal FMS 196: Judgment Fund Award Data Sheet FMS 197: Judgement Fund Voucher for Payment Standard DOC and government forms provided at the time of application for or offer of Federal employment, or at the time

		of onboarding at the DOC. DOC's publication of this Privacy Impact Assessment also serves to provide notice to impacted individuals.
	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: The OSCSP does not directly collect PII, rather, it serves as a document repository and management solution for documents pertaining to legal matters involving Commerce and which may contain PII from other source systems or information collections. Opportunities to decline to provide information may be presented at the original point of collection.

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

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
X	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The OSCSP does not directly collect PII, rather, it serves as a document repository and management solution for documents pertaining to legal matters involving Commerce and which may contain PII from other source systems or information collections. Opportunities to decline to provide information may be presented at the original point of collection.

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: For certain matters, individuals may contact DOC via email, form, letter, or phone and request correction to their information included in documents managed in the LDMS. Additionally, opportunities to access, amend, or correct PII/BII may be available through the source systems from which data is derived, or through means provided under the Privacy Act and as outlined in the applicable SORN.
	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.
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: See Section(s) 5.2 and 8.2 for a discussion of the system's auditing capabilities.
X	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): __**02/12/2021**_ ☐ 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 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 DOC 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 embedded in the Microsoft Office 365 Collaboration Suite and Services. The capabilities provides deep content analysis that helps identify, monitor, and protect PII or BII in the system. DLP helps protect 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 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

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

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

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

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

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-2 – Accounts Receivable COMMERCE/DEPT-14 – Litigation, Claims, and Administrative Proceeding Records COMMERCE/DEPT-18 – Employees Personnel Files Not Covered by Notices of Other Agencies COMMERCE/DEPT-25 – Access Control and Identity Management System OPM/GOVT-10 - Employee Medical File System Records
X	Yes, a SORN has been submitted to the Department for approval on April, 27, 2021. COMMERCE/ DEPT-31, Public Health Emergency Records of Employees, Visitors, and Other Individuals at Department Locations
	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 5.1: Common Office Records - GENERAL RECORDS SCHEDULE 5.2: Transitory and Intermediary Records - Office of the General Counsel - https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-commerce/rg-0040/nc1-040-85-01_sf115.pdf - Office of General Counsel Litigation Case Files - https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-commerce/rg-0040
	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, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
X	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: PII or BII included in documents maintained and managed in the system contain direct identifiers, such as full names, unique identifying numbers such as SSNs, Tax ID/EIN, or other similar, information which directly identifies individuals.
X	Quantity of PII	Provide explanation: Large volumes of PII may be included in documents maintained and managed in the system.
X	Data Field Sensitivity	Provide explanation: PII or BII included in documents maintained in or managed by the system includes information that, if lost, compromised, or disclosed without authorization could result in potential harm, embarrassment, inconvenience, or unfairness to individuals to whom the information pertains or to the Department. However, it is worth noting most information associated with litigation activities included in the system is in the public record after the information has been presented in court.
X	Context of Use	Provide explanation: PII or BII included in documents maintained or managed by the system may be used as part of ongoing litigation involving the Department, or individuals' rights, benefits, or privileges. While the system itself does not process information for this purpose, the information's existence in the system and in certain types of documents impacts

		sensitivity.
X	Obligation to Protect Confidentiality	Provide explanation: For most PII or BII contained in documents maintained in or managed by the system, confidentiality is implied at the original time or point of collection from the subject individual, is required by internal DOC or bureau policy or procedure, or social norms, context, and expectations are such that a reasonable person would assume that information provided is confidential in nature or otherwise protected from unauthorized disclosure or use. In some cases, explicit promises of confidentiality are provided.
X	Access to and Location of PII	Provide explanation: While the system maintains and stores documents locally, limited access outside the Department's headquarters (Herbert C. Hoover Building, or HCHB) with other general counsel staff or attorneys located within Department Bureaus or Operating Units (OUs) will be available. Additionally, system reports may be shared between authorized users outside of the system via secure methods (encrypted email). While a central document management solution reduces the need to share documents outside the system, occasionally, a need to share documents outside the platform may occur. Such sharing will occur, as it current does, via secure means (encrypted email) and only on a need-to-know basis. Access is limited only to internal DOC employees or contractors with a bona-fide need-to-know the information.
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist considering the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made regarding 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.)

This system collects PII. The principal threats, including insider threat, derive from compromised accounts or inappropriate end-user use of data (see element 5.2 above). Controls are in place. BII is the account information itself and typical locator information (room number, address, phone, fax, organization, email).

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.