Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Impact Assessment
for the
Laserfiche Legal Document Management System

Reviewed by: WESLEY FRAVEL, Bureau Chief Privacy Officer

Digitally signed by WESLEY FRAVEL
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=WESLEY FRAVEL, 0.9.2342.19200300.100.1.1=13001003618524
Date: 2018.11.01 09:06:14 -04'00'

☑ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Catrina D. Purvis

Digitally signed by Catrina D. Purvis
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US
Date: 2019.04.19 10:26:03 -04'00'

4/19/2019

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

U.S. Department of Commerce Privacy Impact Assessment
OS/Office of General Counsel / Laserfiche Legal Document Management System

Unique Project Identifier:

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 Laserfiche Legal Document Management System (LDMS) is a Major Application (MA).

(b) System location

The LDMS is hosted within DOC-OGC Network, and housed at the Department of Commerce (DOC or "the Department") headquarters, the Herbert C. Hoover Building (HCHB).

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

As a Major Application, the LDMS sits on the Office of Information Technology Services General Support System (OS-064), which provides an infrastructure backbone for the system. Additionally, the system leverages the DOC "G to G Intranet web Portal" which is the "Government to Government" Intranet DMZ which ensures that only network traffic allowed within DOC (but outside of internal OS, e.g. other DOC bureaus) is able to access the LDMS. "G to G" is used for authentication of users from Bureaus outside OS to the LDMS. Finally, the system leverages common security controls, as do all Office of the Secretary (OS) systems, from the HCHBNet, which is the local area network (LAN) backbone for internal traffic at OS.

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

The LDMS is an enterprise level application that will be used by the Department's Office of General Counsel (OGC) as a document management platform. The LDMS provide a secure repository for maintaining and managing OGC documents pertaining to specific legal matters ("matters") in which the Department is involved. The LDMS will primarily be used for **i)** scoping and defining document searches; **ii)** controlling the way collected documents are submitted to the system, imaged and coded; **iii)** organizing document collections for future

review; and **iv)** producing selected documents using a variety of search criteria. Both electronic and paper documents may be submitted to the LDMS for storage and indexing. Paper documents are electronically scanned and processed with optical character recognition (OCR) software to add machine readable text to the scanned image file. As a result, most documents uploaded to the system are fully keyword searchable. No new information is collected and no existing processes surrounding the original collection and retention of information are changed by the implementation of the LDMS. Scanned documents will continue to be maintained, in hard copy format, in secured, locked file cabinets, or destroyed in accordance with applicable retention requirements.

In addition to documents, LDMS also provides a platform for centralized content storage ranging from image files, to voice and audio files. While most of the file types included in the LDMS will be documents, some attorneys may store audio, voice, or similar files as evidence in support of some legal brief or position, but only on a very sporadic basis and only when necessary. The system will not connect to, access, or otherwise collect from DOC telephonic (voicemail) systems. As necessary, images (generally scans, screenshots, or copies of existing images associated with a specific matter) may also be stored in the system.

The system allows structured and unstructured information to be easily defined and shared across multiple legal teams within the DOC Bureaus and Operating Units (OU). OGC will leverage LDMS to digitize documents and automate document-driven processes, allowing authorized DOC system users to access relevant information in a timely and efficient manner.

OGC's implementation of the LDMS will provide case file management for OGC, including serving as a repository for case histories, notes, and contact information related to legal actions, employment, tort, property, and other matters involving a disbursement of funds and commercial law matters. The LDMS will be available for use by approved OGC employees across the DOC bureaus. Users will access the system via a web version of Laserfiche (web application), which can be accessed from any web browser (IE, Firefox, Chrome, Edge, Safari, etc.) via a DOC network. The features for the web application will mimic a traditional desktop application for end users. Users who are internal to the Office of Secretary (to include HCHB-based employees) networks will access the system via single-sign-on using PIV authentication. Users outside the OS network(s), but on a DOC network, will be provided user IDs and passwords for access to the system, and will access via the existing G to G intranet web portal, and then logging into the application using their provided username and password. A discussion of authorized system users and their permissions, as well as how system access is requested and granted, can be found in Section 6 of this PIA.

While the LDMS is not designed to request or capture Personally Identifiable Information (PII), certain documents and data that are stored and managed through the LDMS in relation to a specific matter may include PII about federal employee/contractors, members of the public, foreign nationals, visitors, or any other party involved in a legal matter with the Department. Data includes contact information and identifying numbers used **i)** in identifying or confirming the identity of personnel, offices, and/or parties in legal actions; **ii)** in ensuring

the proper disbursement of funds in employment, tort, property, and other matters involving a disbursement of funds; and **iii)** throughout the review and analysis of commercial law matters.

Additionally, the LDMS may include PII related to specific, individual matters, such as work-related data like work history, financial information, and demographic data. Section 2 provides additional details on the PII processed by the system.

(e) How information in the system is retrieved by the user

The LDMS allows for retrieval of documents and other data which includes information about specific matters or specific individuals, via a comprehensive keyword search for a word, number, code, title, phrase, or some portion thereof. Such searches could include personal identifiers like names, addresses, or Social Security numbers (SSN), if present in the original documents or data. The tool's advanced capture capabilities perform automated data capture from imported documents, including using OCR software for scanned image files and documents, with index fields completed automatically based on the data extracted.

(f) How information is transmitted to and from the system

Information is transmitted into LDMS in a variety of ways. Each is described in Table 1 below.

TABLE 1 – DATA INPUT METHODS

Method	Description
Browse file and upload	The standard method by which files are uploaded. Users open a "search" window, navigate to and select (a) specific file(s) for upload into the LDMS and choose "Upload." This is also known as the "import dialog box".
Copy and Paste	Allows users to use the standard copy and paste functionality to copy files from a share drive or desktop into the LDMS.
Drag and Drop	Allows users to "grab" a file from a share drive or desktop, by clicking the file and then "dragging" and "dropping" the file into a specific file or dialog box generated by the LDMS.
Snapshot (virtual printer)	Allows users to virtually "print" any document, webpage or screenshot from any application (within DOC networks) and save it directly into the LDMS. Physical printing is disabled.
Microsoft Office Integration	Microsoft Office Integration will be configured for all users with the help of which they will be able to save any files from Office Suite (Word, Excel, Outlook, etc.) directly into LDMS. There will be an option for LDMS within the Ribbon for all office suite products available for saving/uploading documents directly into LDMS.

The most common methods of import are **i)** import dialog box, and **ii)** the drag and drop feature. The "import" dialog box, where users select a series of files for ingest. Both methods allow users to select one or more documents for import. Importing by the "drag and drop" method allows users to import one or more documents at once. Additionally, users may use the "cut and paste" feature in a similar fashion. While the LDMS supports "drag and drop"

functionality for folders, retaining folder structure, DOC's implementation using the web client will not permit this capability.

Less common, but available methods include **i)** Snapshot or virtual printer, which allows virtual "printing" of any document, screenshot or webpage to the LDMS; and **ii)** Microsoft Office integration, which implements a plug-in which appears on the ribbon bar for programs within the Microsoft Office suite that allows users, with one click, to save a file directly to the LDMS.

Regarding dissemination or transmission from the system, the LDMS can produce output in one of two ways – documents or data within the system, in its original form, or reports about those documents or data. The system can share document and metadata related to the documents between different authorized users within DOC OGC, including OGC users across bureaus. Regarding source documents, a user may use a keyword search to find a specific document, "retrieve" that document, then make it available, in accordance with system permissions, to another authorized OGC DOC user for review.

Regarding the generation of reports, the LDMS includes templates, which are comprised of various fields pertaining to certain document types. These metadata fields could be used to generate various reports. For example, a combination of fields "Case Type" and "Date" could help to generate report specific to how many cases of specific type were filed between year 2005 and 2010. Reports are not built about specific individuals within the documents.

(g) Any information sharing conducted by the system

Reports as describe above may be built within the LDMS. Once the reports are built or generated, those reports may be shared with other authorized OGC users within DOC, including across Bureaus and Operating Units (OU). Like source documents, and as described above, reports can be downloaded to a user's local desktop and shared via secure mechanisms (email, share drives) outside the LDMS system. Otherwise, the LDMS does not share information.

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

In general, authority is granted in accordance with the statutes, executive orders, and regulations outlined in DOC Directive (DOO) 10-6. Additionally, the following authorities apply:

- 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

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

Moderate

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

__X__ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*	X	e. File/Case ID	X	i. Credit Card	X
b. Taxpayer ID	X	f. Driver's License	X	j. Financial Account	X
c. Employer ID	X	g. Passport	X	k. Financial Transaction	X
d. Employee ID	X	h. Alien Registration	X	l. Vehicle Identifier	X
m. Other identifying numbers (specify):					

*Explanation for the need to collect, maintain, or disseminate the Social Security number, 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, as amended and all other authorities of the Department.

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

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): See Section 8.2 of this PIA.					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					
The LDMS 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		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					
The LDMS 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		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					
The LDMS 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.

LDMS is a document management tool and it will only be used as a medium to store and manage documents and associated data and files in a centralized location. LDMS 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 LDMS is obtained from DOC bureaus, offices and agency officials and is not verified for accuracy by the LDMS system. The originating DOC bureau or office providing the information for each database is responsible for ensuring the accuracy of information included in the LDMS.

That said, the LDMS features a module called Audit Trail, 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?

	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. **Some information derived from original sources and included in the system may be subject to the Paperwork Reduction Act at the original point of collection.*

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

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

X	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify): Most of the file types included in the LDMS will be documents, however some attorneys could store audio, voice or similar files as evidence in support of some legal brief or position, but only on a very sporadic basis and only when necessary. The system will not connect to, access, or otherwise collect from DOC telephonic (voicemail) systems, nor will the system have the capability to record or create audio recordings.			

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

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters	X	To promote information sharing initiatives	

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).

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 because 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 LDMS:

There is a risk of inappropriate use and protection of information in the LDMS: 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 OGC employees with a clearly defined need-to-know the information. Additionally, the LDMS has an auditing capability that tracks access to each document in the system, including which user accessed the document and when (date and time). Finally, OGC will conduct mandatory training for all LDMS users. The training will include the ways to secure important information and demonstrate how it can be shared with respective stakeholders while maintaining appropriate protection of sensitive information.

There is a risk that the aggregation and "connection" of multiple documents using metadata, as well as the enhanced search capabilities of the system will create new information about individuals: Because information in the system is derived from existing information or documents within and across DOC systems, the centralizing of such information for the purposes of case and document management poses little risk to individual's privacy. Similar capabilities already exist within the systems which currently house such information.

There is a risk that the system may collect or process unnecessary PII: In many cases, documents in the system are subject to legal and regulatory requirements which require that complete document collections be maintained, including documents that contain PII.

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			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify): The LDMS does not share information outside of that which occurs between authorized DOC users as described in Section 6.3 below. As outlined above, reports may be built within the LDMS by authorized users with appropriate permissions to do so. Once the reports are built or generated, those reports may be shared with other authorized users within DOC, including across Bureaus and Operating Units (OU). Reports can be downloaded to a user's local desktop and shared via secure mechanisms (email) outside the LDMS system. Any materials shared with external (to DOC) entities, would include sharing of source documents through processes external to the LDMS (for example, sharing of information related to a particular legal action, on a case-by-case basis with DOJ).			

	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: As noted above, the LDMS is a Major Application housed on the Office of Information Technology Services General Support System (GSS) (OS-064). The OS-064 provides basic backbone infrastructure for the LDMS and the LDMS inherits certain security functions and capabilities from the GSS. 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):			

To request access to OGC's Document Management System, user/s will have to contact their AGC or Chief Counsel. They in turn will then provide details like the DOC employee or contractor's full name, position, proposed access rights (which folders can be visible to them) and privileges (what can they do; scan, read, write, etc.). Once the request has been received by the Systems Administrator, they will create a new user account in the system with proper rights and provide the end user access to LDMS. Each user is assigned a unique account in the LDMS.

Three user roles will exist within the LDMS as described in Table 2 below.

TABLE 2 – LDMS USER ROLES

Role	Description
Full Admin (Administrators – Windows Users)	Includes three (3) system administrators who will have full rights of all the LDMS components and can perform administrative actions that are generally reserved for privileged users, such as creating accounts or granting access or permissions to various users. Administrative accounts are managed by a combination of on-site vendor/contract support and representatives from DOC OGC. Access requests are submitted to identify POCs within DOC OGC and routed for approval by DOC OGC administrators. A vendor's support helpline number and Email will be provided to all end users. The end users can contact the support team with the description of the error/issue and priority.
Super Users (Each Office will have a Super User/s)	Includes one Super User for each office which will perform some basic administrative features like adding/removing features, unchecking checked documents, retrieving deleted documents from recycle

	bin, etc. Super Users can connect directly with Full Admin (System Administrators) or the Support Vendor team to escalate any issues or errors.
Internal (to OS) OGC Users	Includes internal (to the Office of Secretary network) DOC OGC employee users. Users are authenticated using existing internal network authentication methods. User accounts are created, and users are assigned to a group with specific permissions and access by system administrator(s).
External (to OS) OGC Users	Includes external (to the Office of Secretary network) DOC OGC employee users. Users access the LDMS from outside the OS network via DMZ with restricted access (IP authentication). User accounts are created, and users are assigned to a group with specific permissions and access by system administrator(s).

All approved users will have following privileges associated with the specific documents, workflows, or folders, associated with the group into which they are placed, and/or identified at the time of the access request:

- Scan
- Import
- Search
- Print
- Export
- Move Entry
- Process (Enables capabilities to perform OCR, Snapshot, Index and Retrieval of text from an electronic file)

As noted above, each user is assigned an individual, user account and user permissions and access to specific documents or workflows can be configured at a granular level (per user) or per group depending on a specific user's needs.

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
X	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: Privacy Act system warning banner at login/landing page. ___.	
X	Yes, notice is provided by other means.	Specify how: The LDMS 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 LDMS 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 LDMS 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. Consent opportunities for specific uses of implicated data 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 OGC 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. *(Rules of Behavior specific to LDMS outlines confidentiality requirements as a pre-requisite for system access and use).*
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 FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): 10/16/2018 **Note: The system is a child subsystem / Major Application on the OS-064 system. An SSP addendum was completed for OS-064 for the LDMS.* ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
X	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
X	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
X	A security assessment report has been reviewed for the supporting information system and it has been determined that there are no additional privacy risks.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

As a Major Application on the OTIS GSS, the LDMS inherits certain security controls to help endure protection of PII and BII maintained or processed by the system, including:

All OITS-GSS systems employ a multitude of layered security controls to protect PII at rest, during processing, as well as in-transit. These NIST 800-53 controls, at a minimum, are deployed and managed at the enterprise level including, but not limited to the following:

- Intrusion Detection | Prevention Systems (IDS | IPS)
- Firewalls
- Use of trusted internet connection (TIC)
- Anti-virus software to protect host/end-user systems
- HSPD-12 compliant PIV cards
- Access controls

The OITS-GSS systems also follow the National Institute of Standards and Technology (NIST) standards, including special publications 800-53, 800-63, 800-37, etc. Any system within the organization that contains, transmits or processes BII/PII, including the LDMS, has a current authority to operate (ATO) and goes through continuous monitoring on a yearly basis to ensure controls are implemented and operating as intended. The organization also employs data loss prevention (DLP) solutions as well. The DLP is an e-mail scan of unencrypted e-mail traffic, to included attachments, to detect inappropriate transport of sensitive information.

At the application level, the LDMS uses a variety of operational and technical controls to restrict unauthorized access and use. System access is granted only to authorized personnel on an official need to know basis. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels. In addition, all personnel must consent to DOC and system-specific rules of behavior and take annual security and privacy training. The system utilizes Transport Layer Security (TLS) and Secure Socket Layers (SSL) to encrypt internal (OS) network traffic and any traffic over the G2G connection. Further, data is encrypted both at rest and in transit by AES-256 algorithm that is FIPS 140-2 certified.

Regarding the LDMS auditing capability, the capability enables certain authorized users (administrators and other, similar power users) to view, filter, and export audit data stored in binary log files. These users can then create reports to analyze audit data, view the information as a chart, filter it to include only the information relevant to a specific user or users, or specific documents, and export the data for use in spreadsheet programs such as Microsoft Excel. Audit reports include a customizable list of events that have been audited on the LDMS, as well as information about those events. Administrators can choose which events to include in the report and filter the report in several ways, including by time and by user. Reports and report templates can also be saved for future use.

The LDMS also offers reporting about ongoing and completed and unsuccessful workflows pertaining to a specific document managed in the system.

Access controls are in place to limit which employees can gain access and, once access is granted, what documents or materials maintained within LDMS are available to them for viewing or editing, as well as who can upload to a specific folder or group of folders.

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 -2 – Accounts Receivable http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-2.html COMMERCE/DEPT -14 – Litigation, Claims, and Administrative Proceeding Records http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-14.html COMMERCE/DEPT-18 – Employees Personnel Files Not Covered by Notices of Other Agencies http://www.osec.doc.gov/opog/PrivacyAct/SORNs/DEPT-18.html COMMERCE/DEPT-25 - Access Control and Identity Management System http://www.osec.doc.gov/opog/PrivacyAct/SORNs/dept-25.html
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

X	There is an approved record control schedule. Provide the name of the record control schedule: 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	X	Overwriting	X
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.)*

	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.
X	Other:	Provide explanation: Data is unstructured in nature, and no new data collection, including PII, is implicated by the use of LDMS.

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.)

The use of the LDMS raises several privacy risks, including:

There is a risk that individuals may be unaware that their information is maintained or processed within the LDMS, or that they may have limited opportunities to consent to the collection and use of their information in the system: Because the LDMS serves as a document repository and management solution for already existing documents created using information from source systems, some individuals may be unaware, at the original point of collection, that their information is being processed within the LDMS, or may not consent to such processing. In general, this risk is low, because use of the LDMS for document storage and management does not alter any existing business processes relating to the purposes for which information was originally collected, nor does the LDMS use such information to make decisions about an individual's rights, benefits, or privileges. Users are provided opportunities for notice and consent at the original point of collection, by the original method of collection (generally, a form with a Privacy Act Statement). That said, the Department has made this PIA available to serve additional notice of the collection and use of this information by DOC through the LDMS. Notice of the collection and use of information found in documents managed by the LDMS is also available in the applicable SORN as referenced in Section 9 of this PIA.

There is a risk that the system may collect or maintain unnecessary PII or BII, or more information than is necessary for executing DOC OGC's ELI mission: PII and BII may appear in documents related to execution of OGC's ELI mission, and as such, will vary from case-to-case on what PII or BII is included, and may change over time. Documents and data managed within the system are limited to that which is necessary to fulfill the ELI mission as outlined in Section 5.1 above only, and controls exist to limit access and use of the system to those with a clearly defined need-to-know, and to monitor system use. Additionally, DOC has configured the LDMS allow users to redact information, including PII, within documents. Information may be hidden by the document "owner" or user responsible for uploading the document in LDMS, in documents and made available only to specific users based on document access rights or role-based access permissions.

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.

X	Yes, the conduct of this PIA results in required technology changes. Explanation: A warning banner indicating that system contains Privacy Act information was added to the landing/login page. A higher confidentiality impact level (High) for PII resulted in additional controls being implemented to protect PII.
	No, the conduct of this PIA does not result in any required technology changes.