Version Number: 01-2017

U.S. Department of Commerce
Office of the Secretary

Privacy Threshold Analysis
for the
Laserfiche Legal Document Management System

U.S. Department of Commerce Privacy Threshold Analysis

OS/Office of General Counsel / Laserfiche Legal Document Management System

Unique Project Identifier:

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 of the information system in a way that a non-technical person can understand.*

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 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's "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 purpose that the system is designed to serve

DOC 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.

e) The way the system operates to achieve the purpose

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.

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

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.

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

- OGC employees across the DOC bureaus who have requested and been approved for access to the system
- Contractors and DOC employees responsible for administering, securing and managing the system

h) 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.

i) How information is transmitted to and from the system

- **Browse file and upload** – this capability is 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** – this capability 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** – this capability 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.
- **Laserfiche Snapshot (virtual printer)** – this capability allows users to virtually "print" any document, webpage or screenshot from any application (within DOC networks) and save it directly into the LDMS.
- **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.

Questionnaire:

1. What is the status of this information system?

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

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

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System		f. Commercial Sources		i. Alteration in Character	

Management Changes				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 later). *Skip questions and complete certification.*

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

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

____ Yes. *Please describe the activities which may raise privacy concerns.*

__X__ 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 about: *(Check all that apply.)*

__X__ Companies
__X__ Other business entities

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

4. Personally Identifiable Information

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

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

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

__X__ DOC employees
__X__ Contractors working on behalf of DOC
__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 PII other than user ID?

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

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

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

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

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

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

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

CERTIFICATION

__X__ I certify the criteria implied by one or more of the questions above **apply** to the Laserfiche Legal Document Management System 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 [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

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

Joe Mroz (SO)

Signature of ISSO or SO: JOSEPH MROZ Digitally signed by JOSEPH MROZ DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JOSEPH MROZ, 0.9.2342.19200300.100.1.1=13001002958670 Date: 2018.11.02 09:54:07 -04'00' Date: _____

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

Signature of ITSO: Digitally signed by JUN KIM DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=JUN KIM, 0.9.2342.19200300.100.1.1=13001001483988 Date: 2018.11.05 16:28:01 -05'00' Date: _____

Name of Authorizing Official (AO): Terryne Murphy

Signature of AO: TERRYNE MURPHY Digitally signed by TERRYNE MURPHY DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=TERRYNE MURPHY, 0.9.2342.19200300.100.1.1=13001000472785 Date: 2018.11.06 08:50:42 -05'00' Date: _____

Name of Bureau Chief Privacy Officer (BCPO): Wesley Fravel

Signature of BCPO: WESLEY FRAVEL 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 09:08:57 -04'00' Date: _____