

Department of the Interior
Privacy Impact Assessment

March 25, 2013

Name of Project: Laserfiche Document Management System (LDMS)
Major Application (MA)
Bureau: Office of the Secretary (OS)
Project's Unique ID: 010-000000701

A. CONTACT INFORMATION:

Teri Barnett
Departmental Privacy Officer
Office of the Chief Information Officer
U.S. Department of the Interior
1849 C Street N.W.
Mail Stop 5547 MIB
Washington, DC 20240
202-208-1605

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1) Does this system contain any information about individuals?

Yes, the system contains information on Department of the Interior (DOI) employees, contractors, interns, volunteers, and may contain personally identifiable information (PII) on employees of other Federal, tribal, state or local agencies, and individual members of the public. The LDMS contains multiple databases, some of which contain information about individuals and others of which do not. Further descriptions of the databases and the information held by each is provided in section B(2) below.

a. Is this information identifiable to the individual¹?

(If there is **NO** information collected, maintained, or used that is identifiable to the individual in the system, the remainder of the Privacy Impact Assessment does not have to be completed).

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

Yes, information maintained within the LDMS application contains PII. Some information, such as name, social security number and email address is directly identifiable to the individual. Other information, such as office address, bureau, and position title, when used in certain combinations, may permit the identification of an individual. Some of the databases in LDMS contain PII, while others do not. Further descriptions of the databases and the information held by each is provided in Section B(2) below.

b. Is the information about individual members of the public?

(If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security A&A documentation).

Yes, while the bulk of the PII contained in the system will be about employees and contractors of the DOI, some PII will concern members of the public. Some of the databases in the system contain information about individual members of the public, while others do not. Further descriptions of the databases and the information held by each is provided in Section B(2) below.

c. Is the information about employees? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).

Yes, the LDMS application contains information about DOI employees, including full and part time employees, contractors, interns and volunteers. Some of the databases in the system contain information about employees, while others do not. Further descriptions of the databases and the information held by each is provided in Section B(2) below.

2) What is the purpose of the system/application?

The LDMS is an enterprise level application that will be used by the DOI as a document management platform. The LDMS will consolidate several legacy systems and provide a secure repository for Department office documents.

The initial design of LDMS includes five databases that are accessed through a web interface. The five initial databases are:

- **Document Management Unit (DMU).** The DMU will replace DOI's legacy Document Archival Production System (DAPS). The purpose of the DMU database is to manage the process by which DOI responds to requests for production of documents by the courts and Congress, compiles Administrative Records for the Office of the Solicitor, or creates

other document collections. The DMU database is capable of (a) scoping and defining document searches, (b) controlling the manner in which collected documents are submitted to the system, imaged and coded, (c) organizing document collections for future review, and (d) producing selected documents using a variety of search criteria.

Both electronic and paper documents may be submitted to the DMU 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, the majority of documents uploaded to the DMU database are fully keyword searchable.

The DMU database may be used to collect documents or data of any type held by DOI, including documents that contain PII. Because of the expansive scope of the DMU database and the document collections it will hold, it is expected that significant amounts of PII will be collected, including the PII of DOI employees and members of the public.

- **Electronic Library of Interior Policies System (ELIPS).** ELIPS serves as the Department's library of official policies, procedures and programs. ELIPS will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, ELIPS documents may include name and business contact information for various DOI employees. Otherwise, the ELIPS database does not include PII.
- **Office of Surface and Mining Database (OSM Database).** The Office of Surface Mining (OSM) is responsible for regulating active coal mines, reclaiming lands damaged by surface coal mining and abandoned mines, and providing coal mining resources for technical assistance, training, and technology development. The OSM Database will store documents and correspondence related to a variety of OSM's business functions, including project support, permitting, maps, and mining data.

While the majority of documents in the OSM Database will be technical and regulatory in nature and will not contain PII, the OSM Database will collect a moderate amount of PII from OSM employees, as well as the PII of employees of other DOI bureaus and offices, other federal agencies, and state and local officials with any involvement in mining activities. In addition, the OSM Database will contain the PII of members of the public. To cite just a few examples, this may include the names and addresses of private landowners who own property abutting surface mines, or the names of individuals who provide comments regarding specific mining operations or mining permits.

- **Office of the Chief Information Officer Database (OCIO Database).** The Office of the Chief Information Officer (OCIO) coordinates all areas of information management and technology for DOI. The OCIO is currently implementing a series of technological and operational changes and innovations to deliver improved services across the Department at lower costs. One of OCIO's current initiatives, known as IT Transformation, involves restructuring DOI's information technology staffing to better align information technology capabilities with DOI's business and mission areas while reducing overall IT spending. The OCIO Database will contain administrative memorandums and directives related to IT Transformation.
- **Office of Inspector General Database (OIG Database).** The mission of DOI's Office of Inspector General (OIG) is to detect and deter waste, fraud, abuse, and misconduct within DOI programs, and to promote economy, efficiency and regulatory compliance throughout DOI. The OIG Database will provide case file management for OIG, including serving as a repository for case histories, notes, and contact information related to audits, inspections, and civil and criminal investigations.

The OIG Database will store a moderate amount of PII, such as name, title and contact information of OIG and DOI current and former employees and contractors. Certain cases may also involve the PII of other Federal employees, state and local government employees, individuals from Indian tribes, or other members of the general public whose PII may be contained in OIG files.

3) What legal authority authorizes the purchase or development of this system/application?

Departmental Regulations, 5 USC 301; The Paperwork Reduction Act, 44 U.S.C. Chapter 35; the Government Paperwork Elimination Act, 44 U.S.C. 3504; the Clinger-Cohen Act, 40 U.S.C. 1401; OMB Circular A-130, Management of Federal Information Resources; Executive Order 13571, "Streamlining Service Delivery and Improving Customer Service", April 11, 2011

C. DATA in the SYSTEM:

1) What categories of individuals are covered in the system?

DMU - Individuals covered by the system include current and former DOI and other Federal agency employees and contractors, state and local government employees, individuals from Indian tribes, or members of the general public whose PII may be contained in documents submitted to DMU for storage and indexing.

ELIPS – Individuals covered by the system include DOI officials and employees. ELIPS will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, ELIPS documents may include name and business contact information for various DOI employees. Otherwise, the ELIPS database does not contain PII.

OSM Database - Individuals covered in the OSM Database include DOI and OSM employees and contractors whose duties involve surface mining matters. The OSM Database will also contain the PII of members of the public with an interest in or connection to surface mining matters. To cite a few examples, this may include individuals who own property abutting permitted surface mining operations, or individuals who submit comments concerning surface mining permits or surface mining operations.

OCIO Database. The OCIO database will serve as a platform for storing, distributing and viewing memorandums and directives. Individuals whose information is included in the OCIO Database include DOI officials and employees. The OCIO Database will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, OCIO Database documents may include name and business contact information for various DOI employees. Otherwise, the OCIO Database does not contain PII.

OIG Database - Individuals whose PII is included in the OIG Database include current and former employees and contractors of DOI, including OIG personnel. Certain case files may also include the PII of other Federal employees, state and local government employees, individuals from Indian tribes, or other members of the general public whose information may be contained in OIG files.

2) What are the sources of the information in the system?

- a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Information contained within LDMS is obtained from DOI bureaus, agencies, and offices. Information may also be obtained from DOI employees, contractors or volunteers, members of the public, or employees or representatives of other Federal, state, tribal or local agencies. More specifically, the information contained in each of the five existing LDMS databases includes:

DMU – The DMU system collects and stores electronic documents and files, as well as electronic copies of paper files that are held by DOI, its bureaus, agencies or offices, or employees, contractors or agents of DOI.

ELIPS – The source of the information is DOI policy and guidance documents and memoranda generated by DOI bureaus, offices or officials. ELIPS will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials.

OSM Database - Information within the OSM database is collected from OSM records, OSM officials and employees, state and local municipalities and officials, non-governmental organizations that have an interest in surface mining or hold information relevant to surface mining, or members of the public.

OCIO Database – The OCIO Database will be a repository for IT Transformation memorandums and policies and does not collect information directly from individuals.

OIG Database – The primary source of PII in the OIG Database will be records held by DOI, its bureaus and offices that are transferred to OIG case files. Certain case files may also include PII provided by other Federal agencies, Federal employees outside of DOI, state and local government agencies and employees, individuals from Indian tribes, or other members of the general public.

b. What Federal agencies are providing data for use in the system?

DMU – None. The DMU is intended to hold collections of documents and files maintained by DOI and its bureaus and offices. However, some records collected from DOI bureaus and offices during the course of a production of documents may contain data obtained from other Federal agencies in the course of conducting business or through routine correspondence.

ELIPS - The ELIPS database is a repository for the Department’s official policies, including policy and guidance documents and memoranda. Other Federal agencies are not providing data for the ELIPS database.

OSM Database – The OSM Database will hold a wide variety of documents related to surface mining activities, and could potentially include data provided by Federal agencies that perform various activities related to mines, such as the Mine Safety and Health Administration (MSHA), the Environmental Protection Agency (EPA), the Army Corps of Engineers, and the Internal Revenue Service (IRS).

OCIO Database – The OCIO Database is a repository for memorandums and policies and is not expected to hold information from other Federal agencies.

OIG Database – Certain case files contained in the OIG Database may also include data provided by other Federal agencies or Federal employees, and could potentially include any Federal agency with an interest in a matter that is the subject of an OIG case file.

c. What Tribal, state and local agencies are providing data for use in the system?

DMU – The DMU Database may hold data from Tribal, state or local agencies collected from DOI bureaus and offices as part of a production of documents.

ELIPS – None.

OSM Database – The OSM Database may hold information from state and local agencies that have an interest in surface mining matters or hold documents or information that is relevant to specific surface mining projects.

OCIO Database – None.

OIG Database – Certain case files contained in the OIG Database may also include data provided by Tribal, state and local agencies with an interest in a matter that is the subject of an OIG case file.

d. From what other third party sources will data be collected?

DMU – The DMU Database may hold data from third party sources collected from DOI bureaus and offices as part of a production of documents.

ELIPS – None.

OSM Database – The OSM Database may hold information from non-governmental organizations or members of the public that have an interest in surface mining matters or hold documents or information that is relevant to specific surface mining projects.

OCIO Database – None.

OIG Database – Certain case files contained in the OIG Database may also include data provided by non-governmental organizations or members

of the public with an interest in a matter that is the subject of an OIG case file.

e. What information will be collected from the employee and the public?

Information is collected from employees and the public as detailed below for each database. The collection, maintenance and use of the data may be further described in a System of Records Notice (SORN) for each individual database, as identified below.

DMU – Information will not be collected directly from employees or members of the public. With respect to the PII that may be collected, the DMU database can be used to store any document or data file held by DOI. Therefore the database may contain any of the following types of PII: name, social security number, email address, home or work address, telephone contact information, other contact information, gender, age, date of birth, nationality, country of origin, country of citizenship, citizenship status, passport number, driver’s license, passport number, other state or federal government or agency identification number, vehicle registration information, information about personal characteristics such as height, weight, race, employment information, IP address, credit card number, bank account information, or other financial information, health information and related data, information concerning disabilities, criminal background data or history, educational history and information, and information regarding certifications and licenses. Other types of PII that are found in documents or digital files held by DOI may be maintained in the DMU database.

ELIPS – ELIPS will not contain any information on members of the public. Although ELIPS will contain information about employees, the information will not be collected directly from employees. ELIPS will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, ELIPS documents may include name and business contact information for various DOI employees.

OSM Database – OSM may collect information from employees or members of the public that have an interest in surface mining matters or hold documents or information that is relevant to specific surface mining projects. Therefore the database is likely to contain the following types of PII: name, email address, home or work address, other types of data that identify property owned by an individual, such as tax map information, telephone contact information, other contact information, and other state or federal government or agency identification numbers. Other types of PII that are relevant to OSM matters may be contained in the OSM database. Data in the OSM database is covered by several System of

Records Notices, including: Personal Property Accountability Records – Interior, MMS-2; Personnel Security Files – Interior, DOI-45; Employment and Financial Interest Statements – States and Other Federal Agencies, Interior, OSM-8; and Blaster Certification, OSM-12.

OCIO Database – The OCIO Database will not contain any information about members of the public. Although the OCIO Database will contain information about employees, the information will not be collected directly from employees. The OCIO Database will contain copies of policy documents and guidance memoranda that include the name, title and signature of one or more DOI officials. In some cases, the OCIO Database documents may include name and business contact information for various DOI employees.

OIG Database – OIG may request and collect PII from employees or members of the public as needed in the course of conducting case investigations. With respect to the PII that may be collected, the OIG Database will be used by OIG to manage a wide variety of cases. Therefore the database may contain any of the following types of PII: name, social security number, email address, home or work address, telephone contact information, other contact information, gender, age, date of birth, nationality, country of origin, country of citizenship, citizenship status, passport number, driver's license, passport number, other state or federal government or agency identification number, vehicle registration information, information about personal characteristics such as height, weight, race, employment information, IP address, credit card number, bank account information, or other financial information, health information and related data, information concerning disabilities, criminal background data or history, educational history and information, and information regarding certifications and licenses. Other types of PII that are found in documents or digital files relevant to OIG cases may be contained in the OIG database. Data in the OIG Database is covered by two separate System of Records Notices, Management Information – Interior, OIG-1, and Investigative Records - Interior, OIG-2.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOI records be verified for accuracy?

The LDMS application is a document management platform that houses multiple databases and creates copies of documents and existing data for storage in a single centralized repository. Data within each database in the LDMS is obtained from DOI bureaus, offices and agency officials and is not verified for accuracy by the LDMS system. The originating DOI

bureau or office providing the information for each database is responsible for ensuring the accuracy of information entered into the LDMS.

b. How will data be checked for completeness?

The LDMS application is a document management platform that houses multiple databases and creates copies of documents and existing data for storage in a single centralized repository. Data within each database in the LDMS is obtained from DOI bureaus, offices and agency officials and is generally not verified for completeness by the LDMS system. The originating DOI bureau or office providing the information for each database is responsible for ensuring the completeness of information entered into the LDMS.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The LDMS application is a document management platform that houses multiple databases. Data within each database in the LDMS is obtained from DOI bureaus, offices and agency officials; it is the responsibility of the originating DOI bureau or office to ensure that the data entered into the LDMS is current.

The originating bureau or office has the opportunity to delete old documents and upload updated documents to LDMS.

d. Are the data elements described in detail and documented? If yes, what is the name of the document?

Yes, the data elements are described in detail and documented in the Laserfiche Document Management System Security Plan.

D. ATTRIBUTES OF THE DATA:

1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

Yes, the purpose of the LDMS application is to manage electronic documents and the collection and use of PII in several of the LDMS databases is necessary to ensure that certain document collections are complete. In many cases, such as document collections in the DMU and OIG Databases, there are legal and regulatory requirements which require that complete document collections be maintained, including documents that contain PII.

2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?

Documents collected in any of the LDMS databases may be aggregated from different sources. While it is not the intent to create new or previously unavailable data through aggregation, it is possible that new information about individuals may be discerned through the aggregation of documents. Any new information derived from LDMS database information will be in alignment with the purpose of the individual database and the applicable system of records notice.

Each LDMS database is maintained separately with independent access restrictions, and the individual LDMS databases do not share data. Therefore, it is not possible to aggregate data about individuals across the individual databases held in LDMS.

3) Will the new data be placed in the individual's record?

None of the databases in LDMS is intended to create records concerning individuals. All of the documents in LDMS relate to specific matters, such as DMU and OIG document collections, and various matters overseen by OSM. However, it is possible to perform searches on individuals using the database interfaces, and the retrieval of information about an individual from any of the LDMS databases could result in an LDMS user discerning new information about the individual.

4) Can the system make determinations about employees/public that would not be possible without the new data?

The system does not make determinations about employees or the public. In general, LDMS is a document repository and is not used to make determinations or otherwise process data. However, the information in the OIG Database is used to process case files, and the disposition of a case could involve a determination about an individual.

5) How will the new data be verified for relevance and accuracy?

The LDMS application is a document management platform that houses multiple databases and creates copies of documents and existing data for storage in a single centralized repository. Data within each database in LDMS is obtained from DOI bureaus, offices and agency officials and is not verified for accuracy upon or after entry into the LDMS system. The originating DOI bureau or office providing the information for each database is responsible for ensuring the relevance and accuracy of documents included in the LDMS.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

While the LDMS is taking over the operational functions of several legacy systems, the data from each legacy system is being maintained in a distinct database, and no consolidation of data is occurring. Notwithstanding that fact, 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 Departmental rules of behavior and take annual security, privacy and records training in order to obtain and maintain LDMS access.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

Not applicable – processes are not being consolidated.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved in LDMS using keyword searches for a word, number, code, title or phrase (or a portion thereof), including personal identifiers. To the extent that such personal identifiers are present in LDMS, this might include names, email addresses, or social security numbers.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

Each of the LDMS databases can be used to perform searches on individuals using keyword searches for unique personal identifiers such as name. Any user with access to a specific LDMS database can generate a keyword search on individuals. For the most part, the LDMS databases are not intended to generate reports on individuals, with three possible exceptions:

- **DMU Database:** In the course of a litigation matter or Congressional inquiry, it is possible that specific information about an individual will be requested. Reports on individuals will only be produced in response to such inquiries.
- **OIG Database:** In the course of an OIG case or investigation, it is possible that specific information about an individual will be required. Reports on individuals will only be produced in accordance with the applicable System of

Records Notices, Management Information – Interior, OIG-1, and Investigative Records - Interior, OIG-2.

- **OSM Database** – OSM may collect individual information from employees or members of the public that have an interest in surface mining matters or hold documents or information that is relevant to specific surface mining projects. Reports on individuals may be produced, and will be provided pursuant to the routine uses described in the applicable System of Records Notices Personal Property Accountability Records – Interior, MMS-2; Personnel Security Files – Interior, DOI-45; Employment and Financial Interest Statements – States and Other Federal Agencies, Interior, OSM-8; and Blaster Certification, OSM-12.

The LDMS also contains an auditing system which allows reports to be generated on any aspect of its operating controls, which includes all user actions, and the results of both. LDMS system administrators have access to the auditing system, and can run reports on individual system users if necessary to ensure proper use of the system.

10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)

Information is not collected directly from individuals, and individuals do not provide consent to the collection and entry of information into the LDMS. Individual information collected by LDMS is obtained by the originating bureau, office or program prior to entry into LDMS, and individual opportunity to consent to or decline the collection or provision of personal information occurs at the time of collection by the originating bureau, office or program.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

The primary system is being maintained at a single site. The primary site will be mirrored to a secondary site for backup purposes or to provide coverage in the event of a significant outage of the primary system. Absent a significant outage, all data transfer will be unidirectional from the primary server to the backup server. No additional data collection will occur on the backup server. As a result, the data in each location will be consistent. In the event that the backup server is used to run the system during an extended outage period, specific automated controls are in place to ensure the complete transfer of all collected data back to the primary server.

2) What are the retention periods of data in this system?

Records for each of the LDMS databases are maintained in accordance with the applicable records schedule for the bureau or agency managing the database, and compliance with the records schedules remains a bureau and agency responsibility.

DMU - Records are retained in accordance with Office of the Secretary Records Schedule 2501, Litigation Document Production Administrative Files. The disposition is temporary. Retention of congressional document production and administrative files will be cut off at the end of each document production and destroyed 8 years after cut-off. Retention of litigation document production and administrative files will be cut off at the end of each document production and destroyed 6 years after cut-off. A records retention schedule for miscellaneous collections is being developed and will be submitted to the National Archives and Records Administration (NARA) for scheduling and approval. Pending approval by NARA, these documents will be treated as permanent records.

ELIPS - Documents are maintained in accordance with Departmental Records Schedules (DRS) 6201-Departmental Manual Files which are permanent, are cut off at the end of the calendar year, and transferred to NARA 20 years after the cut off; 6202-Succession Memoranda files which are temporary, are cut off when superseded, and destroyed 6 years after they are cut off; and 6203-Secretarial Order Files are permanent, are cut off at the end of the calendar year, and transferred to NARA 20 years after the cut off.

OSM Database – Records in the OSM Database are covered by General Records Schedule NC1-433-80-1. GRS NC1-433-80-1 covers a wide range of records, and retention schedules vary based upon record type.

OCIO Database – Documents are maintained in accordance with Departmental Records Schedules (DRS) 6201-Departmental Manual Files which are Permanent, are cut off at the end of the calendar year, and transferred to NARA 20 years after the cut off; 6202-Succession Memoranda files which are temporary, are cut off when superseded, and destroyed 6 years after they are cut off; and 6203-Secretarial Order Files are permanent, are cut off at the end of the calendar year, and transferred to NARA 20 years after the cut off.

OIG Database – Documents are maintained in accordance with Departmental Records Schedules (DRS) 2802, Office of the Inspector General – Investigative Records. Disposition for investigative records selected for their continued historical value are permanent, and cut off at the end of the fiscal year in which investigation is concluded, with transfer to NARA 25 years after cut-off; disposition for all other investigative records is temporary, and

cut off at end of fiscal year in which investigation is concluded; destroyed 10 years after cut off.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Records are disposed of in accordance with the applicable Departmental records retention schedule, Departmental policy and NARA guidelines. Paper records are disposed of by shredding or pulping, and records contained on electronic media are degaussed or erased in accordance with 384 Department Manual 1.

- 4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

- 5) How does the use of this technology affect public/employee privacy?**

The LDMS is a cloud-based enterprise application that will be used by the DOI as a document management platform. The databases within the LDMS hold large amounts of PII which poses some risk to the privacy of employees and members of the public. However, these risks are mitigated by the security controls identified below.

Cloud technology - The LDMS will be hosted by a Federal Information Security Management Act (FISMA) compliant cloud services vendor. The LDMS will be hosted by a cloud provider that will be required to comply with all relevant NIST standards. A formal Assessment and Authorization (A&A) of the system will be completed to ensure security and privacy impacts from the use of the system are effectively reduced and managed. Furthermore, the LDMS will be hosted by an American-based cloud services host at a facility located in Virginia, so there will be no jurisdictional concerns about the maintenance of the data that can arise when cloud-based systems are hosted offshore.

Enterprise application – Enterprise applications supporting multiple databases may raise concerns about maintaining security across the databases to ensure that there is no improper sharing of information. However, the databases in the LDMS are segregated and secured to prevent unauthorized information sharing, and each database is accessed through a unique interface point. LDMS users are granted limited rights, based on the concept of least privilege, and the LDMS contains an audit trail feature to monitor use and prevent misuse of the data in the system.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

The LDMS has an audit log that can be used to run reports on individual users' access to and actions within the LDMS. Additionally, the LDMS contains a user traceability program that can detect unauthorized access attempts or access to files outside of an authorized user's permissions.

Otherwise, the purpose of the LDMS is to serve as a document management system, and does not have the capability to identify, locate and monitor individuals.

7) What kinds of information are collected as a function of the monitoring of individuals?

The LDMS audit log can be used to run reports on individual users' access to and actions within the LDMS, such as date and time of day a user accessed the system, specific web pages accessed, search terms or parameters used to call data from the LDMS's database, user creation and deletion of files, user creation or deletion of user accounts, and changes to account privileges. The user traceability program can detect and report unauthorized access attempts to files outside of an authorized user's permissions.

8) What controls will be used to prevent unauthorized monitoring?

Only authorized users who have been given a username and password will be able to access the system. In addition, all users must complete Federal Information System Security Awareness (FISSA), Privacy and Records Management training before being granted access to any DOI IT resource, and annually thereafter.

The audit trail feature, unique identification, authentication and password requirements, along with mandatory security, privacy and records management training requirements, help prevent unauthorized monitoring, as well as unauthorized access to data, browsing and misuse.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

The databases within the LDMS are managed by bureaus and offices with individual Privacy Act Systems of Records Notices: Management Information – Interior, OIG-1; Investigative Records - Interior, OIG-2; Personal Property Accountability Records – Interior, MMS-2; Personnel Security Files – Interior, DOI-45; Employment and Financial Interest Statements – States and Other Federal Agencies, Interior, OSM-8; and Blaster Certification, OSM-12.

DOI System of Records Notices may be viewed at:
http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm.

10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

The system is not being modified.

F. ACCESS TO DATA:

1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Authorized DOI managers, system administrators, and authorized users will have access to the data in LDMS. Access to each LDMS database is restricted to system administrators and user access is granted to each database separately. User access is based on the concept of least privileges, granting users only the lowest levels of access rights needed to perform their job functions. Contractors and system developers may have access to relevant portions of the system for limited periods of time for system development, modification, or enhancement.

The Department of Justice will review documents contained within the DMU document production files collected in preparation for litigation in order to perform attorney review in conjunction with DOI Office of the Solicitor.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is granted to each individual database in LDMS, and the originating bureau, agency, or office for each database will have the ability to determine the standards and procedures for granting access to their database. In general, access will be granted on a case by case basis and will depend on job function and a need to have access to the requested information. Individuals requesting access to each database in the system must fill out the LDMS Access Request Form, which must be signed by a supervisor responsible for the database. The supervisor will indicate the level of access to be granted.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Users will be granted access only to a specific database, with further restrictions on the documents and files that may be accessed, based on job function and need to know. The LDMS has technical controls in place to restrict access beyond the user's assigned role.

- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

The LDMS system has multiple layers of security that protect content to the object level and can be applied to a user, group of users, or set as a general feature. Account access within the LDMS is also limited in that users have a defined time period during which their access is actually active. This automatic feature will log out inactive users and disable their user account based on their access needs. The LDMS can generate both usage and customized access reports that will report users who have been inactive or disabled from the system as needed.

Additionally, the LDMS contains a user traceability program that can detect unauthorized access attempts or access to files outside of a user's permissions. The audit trail feature, unique identification, authentication and password requirements, and mandatory security, privacy and records training requirements help prevent unauthorized access to data, browsing and misuse.

- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?** If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Contractors are providing a variety of design, development and system maintenance services, and Privacy Act contract clauses were inserted in their contracts and all regulatory matters were addressed.

- 6) Do other systems share data or have access to the data in the system? If yes, explain.**

No.

- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The LDMS System Administrator will have the ultimate responsibility for protecting the privacy rights of the public and employees affected by the interface.

- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

The Department of Justice will have access to the DMU document production files collected in preparation for litigation through secured point-to-point web

connection in order to perform attorney reviews in conjunction with DOI Office of the Solicitor. Otherwise, other agencies will not have access to LDMS data.

9) How will the data be used by the other agency?

The Department of Justice will review documents contained within the DMU document production files collected in preparation for litigation in order to perform attorney review in conjunction with DOI Office of the Solicitor.

10) Who is responsible for assuring proper use of the data?

The LDMS system manager, LDMS information system security officer, and each database system manager will be responsible for the proper use of the system and the data.