Criminal Division

Privacy Impact Assessment
for the
Litigation Support System

Issued by:
Jennifer A.H. Hodge
Criminal Division, Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: August 17, 2022

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The U.S. Department of Justice, (Department or DOJ), Criminal Division (Division) develops, enforces, and supervises the application of all federal criminal laws, except those specifically assigned to other Divisions and certain civil litigation.

In the performance of these duties, Division employees handle massive quantities of information and must ensure that information is handled in compliance with the legal and privacy rights of defendants, complainants, and other requestors of information. Whether they be discovery packages for litigation, privilege reviews, large volume Freedom of Information Act (FOIA) or Privacy Act (PA) requests, subpoena responses, records preservation requests, internal administrative inquiries, or another category of materials, Division employees frequently encounter the need to review, analyze, process, categorize, redact, and produce large volumes of materials. These materials may include paper documents, a vast variety of electronic documents, and forensic images of computers, compact discs, thumb drives, and other media.

In document-intensive cases, or cases where electronic documents must maintain forensic integrity, Division personnel will conduct the discovery process through electronic means, in a process commonly referred to as "eDiscovery." The Division maintains a suite of software packages and applications for the purpose of meeting its document management and review needs, which are collectively referred to as the "Litigation Support System (LSS)." The Division conducted this Privacy Impact Assessment to assess and mitigate the risks to the Personally Identifiable Information (PII) collected in this system, which includes large volumes of materials with amalgamations of PII.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

In criminal cases, courts compel full and open discovery of all relevant agency records to the defendant, via the Fifth and Sixth Amendments to the U.S. Constitution and the Federal Rules of Criminal Procedure.[1] In civil cases, the Federal Rules of Civil Procedure[2] govern most discovery requirements, which the federal courts may enforce. Both civil and criminal cases may require Privilege Review,[3] for the exclusion from the

---

[1] Fed. R. Crim. P. (2020), *see* https://www.federalrulesofcriminalprocedure.org/table-of-contents/.
[2] Fed. R. Civ. P. (2020), *see* https://www.federalrulesofcivilprocedure.org/.
[3] According to LexisNexis, "Privilege Review is the stage at which all of the documents initially tagged as "Privileged" during the document review will be subject to closer scrutiny and at which a final determination is made as to whether or not the document is subject to privileged status." *See* https://www.lexisnexis.com/legalnewsroom/legal-business/b/strategy/posts/are-attorneys-properly-prepared-for-

prosecutor of documents that violate a defendant's legal rights. Discovery productions can require the preservation, collection, and analysis of large volumes of electronic documents in a variety of formats, as well as audio files and forensic copies of computers, hard drives, or other electronic media (for purposes of this PIA, audio files and forensic copies will be generically referred to as documents). Additionally, large volumes of documents may be collected pursuant to subpoenas.

Additionally, although FOIA and Privacy Act requests are less frequent than litigation cases, the processing of these sometimes-large volume requests involves the same processes of determining responsiveness and searching, analyzing, coding, and redacting as necessary for an eDiscovery package. Division employees may also need to expedite other mission-related or administrative document-processing needs, such as records preservation requests or internal administrative inquiries.

The Division facilitates these large volume productions through a suite of commercial, off-the-shelf eDiscovery software packages, including Relativity, Nexedia, Nuix, and similar supporting technologies. Requests for uploading, processing, indexing, creating forensic images, and generating packages for production and case workflow are managed through a customized database. These software packages, taken together with customized database, are jointly referred to as the Litigation Support System (LSS) and are managed by employees and contractors of the Automated Litigation Support Unit (ALS). These tasks handled by LSS typically include:

- Processing information in a secure and forensically sound manner, including electronic, audio, and non-electronic (e.g., paper) information;
- Analyzing and processing information, including forensic images of electronic devices and data retrieval, as well as formatting and organizing information for easy search, retrieval, review, coding, annotation, and presentation;
- Reviewing information, including searching, retrieving, reviewing, coding, annotating, and organizing information;
- Redacting PII, privileged information, or information exempt from or pursuant to the FOIA/PA;
- Producing responsive documents to meet litigation discovery requirements, subpoena responses, FOIA/PA requests, or expert-witness pre-trial review; and
- Presenting information, including processing, formatting, and organizing information for discovery and/or trial exhibits.

The documents loaded into LSS are often unaltered copies of existing data that are already stored in other paper-based or electronic recordkeeping systems maintained by the Division. These can include, but are not limited to, case files, evidentiary items included as part of Division case files, Division e-mail accounts, or other systems of information subject to FOIA/PA disclosures. Pursuant to statutory authorities, the Division has collected and preserved this information manually for many decades. LSS

---

privilege-review.

does not constitute a new type or purpose of collection; instead, it provides an electronic enhancement to this previously manual process, improving both accuracy and efficiency.

In order to manage, review, and produce large volumes of documents, exact copies of the pertinent documents are gathered from the Division's systems at the direction of the case attorney. These documents are then loaded into LSS by ALS. Where necessary, evidence in the form of images of electronic devices may be obtained through the appropriate chain of custody from the investigating agency and loaded directly into the system, in order to satisfy the Best Evidence Rule of criminal procedure. Relativity and Nuix then extract text and metadata and convert them to a user-friendly format for efficient document management. Specifically, these applications include functionality for analyzing, culling, reviewing, searching, de-duplicating, and producing potential evidence. The documents are then loaded into an electronic case file in Relativity or Nexidia, which provides CRM staff the ability to automate, review, analyze, redact, and conduct other functions associated with preparing discovery/document packages. These functions include:

- Managing a variety of file formats, for example: Microsoft product formats, image formats, Adobe formats, audio files, CAD files, Vector files, e-mails, HTMLs files, and many more. End users view the majority of the formats through a software viewer. File types not supported by the viewer can be viewed in the original application stored on the end user's computer;
- Reviewing the metadata stored within the file in a user-friendly format;
- Identifying and allowing the option for de-duplication for a more efficient review process;
- Automating the identification of critical information by searching for names, phrases, and terms (collectively, "keywords") that the reviewing attorney identifies and tags responsive documents for further review. Keyword tags may indicate the existence of responsive, privileged, or personally identifiable information;
- Allowing bulk electronic redaction of words, terms, pages, or regions of a page, in a fashion that overlays temporary redactions on documents within LSS, but makes them permanent in the final production package, so that altered redactions can be produced as may be required by the courts;
- Creating new information that is associated with those records in order to protect the integrity of the original records. The LSS-created data consists of redactions; tags; privilege logs created by the LSS software; search and filter reports; and an audit trail, which LSS automatically creates and maintains as an historical record of actions users take in each case to the extent required by the National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4;[4]
- Allowing for a privilege review team to wall-off privileged documents from a prosecutorial team;

[4] *See* https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22.

- Allowing the user to enter free-form text notes describing the reason for the redaction; and
- Allowing LSS to generate reports based on the search terms and filters that were used to withhold records to demonstrate a defensible process for gathering the totality of relevant data.

Once the Division staff completes the above-described automated review process, they then perform a final manual review to verify the accuracy and appropriateness of redacted and unredacted information, as warranted by the case. When the files are approved, ALS places the reviewed records in the appropriate file format for production. The production packages are provided to the appropriate party such as defense counsels or the information requestors.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	**Citation/Reference**
☒ Statute	44 U.S.C. § 3101; 5 U.S.C. § 552; 5 U.S.C. § 552a; 5 U.S.C. § 30; 28 U.S.C. §§ 516, 519
☐ Executive Order	
☒ Federal Regulation	28 C.F.R. §§ 0.55 through 0.64–5
☐ Memorandum of Understanding/agreement	
☒ Justice Manual[5]	Title 9: Criminal: 9.5
☒ Other (summarize and provide copy of relevant portion)	Fifth and Sixth Amendments to the U.S. Constitution, Federal Rules of Criminal Procedure, Federal Rules of Civil Procedure

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

[5] https://www.justice.gov/jm/justice-manual.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Individuals Outside DOJ; C. US Citizens or Lawful Permanent Residents (USPERs); D. Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Website will collect email addresses of individuals outside DOJ who could be US or non-USPERs*
Name	X	A,B,C,D	* See Note Below
Date of birth or age	X	A,B,C,D	* See Note Below
Place of birth	X	A,B,C,D	* See Note Below
Gender	X	A,B,C,D	* See Note Below
Race, ethnicity or citizenship	X	A,B,C,D	* See Note Below
Religion	X	A,B,C,D	* See Note Below
Social Security Number (full, last 4 digits or otherwise truncated)	X	A,B,C,D	* See Note Below
Tax Identification Number (TIN)	X	A,B,C,D	* See Note Below
Driver's license	X	A,B,C,D	* See Note Below
Alien registration number	X	A,B,C,D	* See Note Below
Passport number	X	A,B,C,D	* See Note Below
Mother's maiden name	X	A,B,C,D	* See Note Below
Vehicle identifiers	X	A,B,C,D	* See Note Below
Personal mailing address	X	A,B,C,D	* See Note Below
Personal e-mail address	X	A,B,C,D	* See Note Below
Personal phone number	X	A,B,C,D	* See Note Below
Medical records number	X	A,B,C,D	* See Note Below
Medical notes or other medical or health information	X	A,B,C,D	* See Note Below
Financial account information	X	A,B,C,D	* See Note Below
Applicant information	X	A,B,C,D	* See Note Below
Education records	X	A,B,C,D	* See Note Below
Military status or other information	X	A,B,C,D	* See Note Below
Employment status, history, or similar information	X	A,B,C,D	* See Note Below
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A,B,C,D	* See Note Below
Certificates	X	A,B,C,D	* See Note Below
Legal documents	X	A,B,C,D	* See Note Below
Device identifiers, e.g., mobile devices	X	A,B,C,D	* See Note Below
Web uniform resource locator(s)	X	A,B,C,D	* See Note Below
Foreign activities	X		* See Note Below
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A,B,C,D	* See Note Below
Juvenile criminal records information	X	A,B,C,D	* See Note Below
Civil law enforcement information, e.g., allegations of civil law violations	X	A,B,C,D	* See Note Below

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Individuals Outside DOJ; C. US Citizens or Lawful Permanent Residents (USPERs); D. Non-USPERs	(4) Comments
Whistleblower, e.g., tip, complaint or referral	X	A,B,C,D	* See Note Below
Grand jury information	X	A,B,C,D	* See Note Below
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A,B,C,D	* See Note Below
Procurement/contracting records	X	A,B,C,D	* See Note Below
Proprietary or business information	X	A,B,C,D	* See Note Below
Location information, including continuous or intermittent location tracking capabilities	X	A,B,C,D	* See Note Below
Biometric data:			
- **Photographs or photographic identifiers**	X	A,B,C,D	* See Note Below
- **Video containing biometric data**	X	A,B,C,D	* See Note Below
- **Fingerprints**	X	A,B,C,D	* See Note Below
- **Palm prints**	X	A,B,C,D	* See Note Below
- **Iris image**	X	A,B,C,D	* See Note Below
- **Dental profile**	X	A,B,C,D	* See Note Below
- **Voice recording/signatures**	X	A,B,C,D	* See Note Below
- **Scars, marks, tattoos**	X	A,B,C,D	* See Note Below
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A,B,C,D	* See Note Below
- **DNA profiles**	X	A,B,C,D	* See Note Below
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A	
- **Queries run**			
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible): _____ _____ _____			

* All of the listed information could conceivably be captured in Division Case Files. which may be subject to discovery, FOIA/PA, or other requests. The presence of the information is

entirely dependent on the circumstances of each individual matter. The information would relate to the defendant(s) in a case or the subject(s) of other types of information requests. None of the information listed above is specifically solicited by this system, but to the extent it is present within information gathered, it can be indexed and searched by these programs.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from individual about whom the information pertains		
☒ In person	☒ Hard copy: mail/fax	☒ Online
☐ Telephone	☒ Email	
☒ Other (specify): Hard Drive or CD		

Government sources		
☒ Within the Component	☒ Other DOJ components	☒ Other federal entities
☒ State, local, tribal	☒ Foreign	
☐ Other (specify):		

Non-government sources		
☒ Members of the public	☐ Public media, internet	☒ Private sector
☐ Commercial data brokers		
☐ Other (specify):		

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	☒	☐	☒	Sharing will consist of discovery packages for litigation, privilege reviews, large volume Freedom of Information Act (FOIA) or Privacy Act (PA) requests, subpoena responses, records preservation requests, or internal administrative inquiries.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
				Access to this system is limited based on a need-to-know, and further limited to the minimum access needed.
DOJ Components	☒	☐	☒	Sharing will consist of discovery packages for litigation, privilege reviews, large volume Freedom of Information Act (FOIA) or Privacy Act (PA) requests, subpoena responses, records preservation requests, or internal administrative inquiries. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed.
Federal entities	☒	☐	☒	Sharing will consist of discovery packages for litigation, privilege reviews, large volume Freedom of Information Act (FOIA) or Privacy Act (PA) requests, subpoena responses, or records preservation requests. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed.
State, local, tribal gov't entities	☒	☐	☒	Sharing will consist of discovery packages for litigation, privilege reviews, subpoena responses, or records preservation requests. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed.
Public	☒	☐	☐	Sharing will be for FOIA/PA requests.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	Sharing will consist of discovery packages for litigation, privilege reviews, large volume Freedom of Information Act (FOIA) or Privacy Act (PA) requests, subpoena responses, or records preservation requests.
Private sector	☐	☐	☐	
Foreign governments	☐	☐	☐	
Foreign entities	☐	☐	☐	
Other (specify):	☐	☐	☐	

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Litigation and investigative information will not be released to the public for "Open Data" purposes. Information which is the subject of FOIA and/or PA requests will be released to the requestor, if appropriate, after application of the exemptions under the appropriate statute.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The public is provided with general notice of the existence of case files through the:

- Division System of Record Notice (SORN) JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24151, 155 (May 25, 2017); and
- JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), and amended at 82 Fed. Reg. 24151, 152 (May 25, 2017).

Generally, individuals are not provided with specific or direct notice of law enforcement-related information collections about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals are provided with general notice of the existence of case files through the System of Records Notice, Central Criminal Division Index File and Associated Records, JUSTICE/CRM-001.

Generally, individuals may not be provided with the opportunity to voluntarily participate in law enforcement-related information collections about themselves, or consent to such collections or specific uses of such information, if it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

An individual may request access, amendment, and/or correction to information pertaining to them by following the procedure as published on the Division website[6] and described in the relevant Systems of Records Notices.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** Litigation Support System – LSS – CSAM ID 1606 - ATO valid until 12/10/2022. **If an ATO has not been completed, but is underway, provide status or expected completion date:** **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** LSS has undergone assessments, penetration tests, and vulnerability scans, and is monitored by other means by the CRM Information Systems Security Officer.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The Division collects logs according to the standards in the DOJ Cybersecurity Standards, which include Operating System, Web, Database, and Application logs for every FISMA-applicable system. Logs are correlated into appropriate DOJ information systems managed

[6] *See* https://www.justice.gov/criminal/crm-freedom-information-act

	by Justice Management Division (JMD). Access to these logs is provided to the Justice Security Operations Center (JSOC) to conduct security analysis and log monitoring for unusual activity to the extent required by NIST SP 800-53. Information owners or stewards that identify additional audit review requirements per the NIST control selections in their System Security Plan and further defined by entries in a Continuous Monitoring Implementation Plan (CRM Template) can have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the information owner.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** One-on-one and case-specific training, specific to this system, is conducted for newly authorized users, including contractors.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

All Division systems implement technical controls to reduce the risk of compromise to PII. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- LSS has a security categorization of FISMA Moderate and has selected the applicable security controls for a Moderate baseline. The Division will not input any information that would be categorized as "High" under NIST FIPS Publication 199, or NIST SP 800-60, Volume II, into this system without the approval of appropriate privacy and security personnel, to ensure adequate controls are applied to protect such information.
- LSS is accessible by approved DOJ employees, contractors, and select attorneys and law enforcement from other Federal agencies only, and on case-by-case bases. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed. It utilizes "tiered," role-based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to

perform the job, and is individually verified through the employee's PIV card.

- LSS is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- As described throughout this PIA, all LSS users, including the select attorneys and law enforcement from other Federal agencies, must complete annual DOJ Computer Security Awareness Training (CSAT) training, as well as read and agree to comply with DOJ information technology Rules of Behavior. LSS system administrators must complete additional professional training, which includes security training.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered, role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.
- Outside access for other Federal law enforcement or litigation personnel is centralized through the Law Enforcement Enterprise Portal (LEEP) maintained by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services Division (CJIS) on a case-by-case basis. Access will be granted to federal prosecutors and law enforcement personnel in the performance of their duties and is verified through their PIV credentials. Access through LEEP may be granted to state or local prosecutors or law enforcement personnel who have a verified need to access the system and pass a vetting process integrated into LEEP by CJIS. Access to this system is limited based on a need-to-know, and further limited to the minimum access needed.

Overall, LSS's defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby mitigating the consequences should a breach occur.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Disposition of records within LSS will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of hardcopy and softcopy records. Documents are not retained within LSS once processing has completed, and are returned to their source.

Documents processed for criminal investigations are received from and returned to the Division's investigative case file. As relates to their retention in those case files, retention is controlled by the case file retention requirements listed in Department Retention Schedule N1-60-88-10 (https://www.archives.gov/files/records-

mgmt/rcs/schedules/departments/department-of-justice/rg-0060/n1-060-88-010_sf115.pdf), which is generally 10 years after the close of the case unless otherwise defined in the records schedule.

Documents processed for FOIA purposes are received from and returned to the Division's FOIA file. As relates to their retention in those case files, retention is controlled by the case file retention requirements listed in General Records Schedule 4.2 (https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf) which are generally retained for 3 years absent an intervening business use.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

☐ No. ☒ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

- System of Records Notice JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007 and amended at 82 Fed. Reg. 24155 (May 25, 2017).
- System of Records Notice JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021).
- System of Records Notice JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), and amended at 82 Fed. Reg. 24151, 152 (May 25, 2017).

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention***

schedules),

- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The Division undertakes a number of measures to mitigate the risk of the unauthorized access to, and resulting potential misuse of information. DOJ employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access-restricted office suites. LSS also implements access monitoring, and privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

Employee access to LSS is limited based on a need-to-know and further limited by restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's Personal Identity Verification (PIV) card and pin number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by the Federal Information Security Modernization Act of 2014 (FISMA). As described in section 6, an audit log is maintained of user logins and actions, to the extent required by NIST SP 800-53. Notification of the monitoring is presented clearly when logging into the system.

Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's CSAT, as well as read and agree to comply with DOJ Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with DOJ, and annually thereafter. Additionally, ALS provides training for employees granted access to LSS. The Division maintains an Account Management Guide and Configuration Management Guide for LSS.

The IT system assessment is documented in the DOJ CSAM assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan for LSS. There is no outside administrative access to this system; instead, administrator access is restricted to the few DOJ employees and contractors who administer the program.

The Division undertakes various measures to mitigate the risk of name association with LSS. As in most cases where a record associates a person with a criminal investigation, the mere presence of a name in the system can generate the assumption of involvement with criminal activity or other damage to their reputation. For this reason, there is no automated dissemination of information from this system outside of the Division or the approved users from other Federal agencies. Any dissemination must be done pursuant to proper authority and management review.

To mitigate the risk of over-collection of information, the Division makes every effort to diligently review, verify, and appropriately include or exclude information from this system. Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. This system is a means to analyze unstructured data, in order to determine what is relevant to an investigation or inquiry, or in other words, what is and is not over-collection. It will, by its nature, over-collect information, for example, the contents of an entire computer hard drive obtained through a legally obtained and executed search warrant. The automated text searches, tagging, and redaction functions are specifically designed to identify whether information is relevant to the matter at hand so that the remainder can be excluded.

The Division also relies on the training and subject-matter expertise of the users to appropriately apply the Federal Rules of Criminal and Civil Procedure, as well as the FOIA and PA regulations in determining whether collected information is relevant and appropriate. Both the investigating agencies and DOJ verify this information as part of the normal procedures associated with day-to-day tasks, which include multiple levels of oversight and review.