

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: Michelle Ramsden
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: October 8, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The U.S. Department of Justice, (Department or DOJ), Criminal Division (Division or CRM) 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, smart devices, social media messaging and other digital 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, applications, and cloud services for the purpose of meeting its document eDiscovery needs, which are collectively referred to as the “Litigation Support System (LSS).” In order to maintain technological capabilities current with the evolving digital landscape, the Division occasionally adds new components to its LSS suite. The Division is doing so at this time, as noted in the attached Appendix. The Division conducted this Privacy Impact Assessment (PIA) 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 Procedure² 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 prosecutor, of documents that

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”

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 or other legal process.

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 (further described in the appendix). Requests for uploading, processing, indexing, creating forensic images, and generating packages for production and case workflow are managed through a customized internally developed database. These software packages, taken together with customized database, are jointly referred to as LSS and are managed by employees and embedded contractors of the Automated Litigation Support Unit (ALS). These tasks handled through 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 does not constitute a new type or purpose of collection.

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-privilege-review>.

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 supervising end user (end users include case attorneys, case team members, FOIA/PA processors, privilege review team members, executors of administrative records requirements or records preservation orders). These documents are then loaded into LSS by ALS, who then works with the end-users to ensure that the specific needs of their request are met. 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. ALS employees will then extract text and metadata and convert them to a user-friendly format for efficient document management. Finally, a quality control process is conducted to ensure the usability of the documents and functionality of the documents for the end-user review. 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 options for and applying 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 approved 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; search and filter reports; and an audit trail, which LSS automatically creates and maintains as an historical record of actions end-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
- Creating access controls to define the access level of the case team and allowing for a privilege review team to wall-off privileged documents from the case team;
- Allowing the user to enter free-form text notes describing the reason for the redaction or relevant facts; 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.

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

Once the end-users complete 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
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> Executive Order	
<input checked="" type="checkbox"/> Federal Regulation	28 C.F.R. §§ 0.55 through 0.64–5
<input type="checkbox"/> Memorandum of	
<input checked="" type="checkbox"/> Justice Manual ⁵	Title 9: Criminal: 9.5
<input checked="" type="checkbox"/> 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 See <https://www.justice.gov/jm/justice-manual>

Department of Justice Privacy Impact Assessment

Criminal Division/Litigation Support System

Page 5

(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 Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
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
Professional mailing address	X	A, B, C, D	* See Note Below
Professional e-mail address	X	A, B, C, D	* See Note Below
Professional phone number	X	A, B, C, D	* See Note Below
Social Media Identifiers	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

Department of Justice Privacy Impact Assessment

Criminal Division/Litigation Support System

Page 6

(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 Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Foreign activities	X	A, B, C, D	* 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
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)	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. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
<i>System admin/audit data:</i>	X	A	This system captured audit data as mandated in National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4. ⁶
- User ID	X	A	
- User passwords/codes			
- IP address			
- Date/time of access	X	A	
- Queries run			
- Contents of files	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Given the varied nature of the Division's work, the information placed into LSS could include any type of lawfully obtained, unclassified information reasonably determined by the Department to be necessary and/or relevant to a law enforcement investigation.

* 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		
<input checked="" type="checkbox"/> In person	<input checked="" type="checkbox"/> Hard copy: mail/fax	<input checked="" type="checkbox"/> Online
<input type="checkbox"/> Telephone	<input checked="" type="checkbox"/> Email	
<input checked="" type="checkbox"/> Other (specify): Digital devices, information or communications		

Government sources		
<input checked="" type="checkbox"/> Within the Component	<input checked="" type="checkbox"/> Other DOJ components	<input checked="" type="checkbox"/> Other federal entities

⁶ See <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22>.

☒ 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			Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
	Case-by-case	Bulk transfer	Direct log-in access	
Within the Component	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sharing will consist of discovery packages for litigation, privilege reviews, large volume FOIA/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.
DOJ Components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sharing will consist of discovery packages for litigation, privilege reviews, large volume FOIA/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.

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.
Federal entities	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sharing will consist of discovery packages for litigation, privilege reviews, large volume FOIA/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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sharing will be for FOIA/PA requests.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sharing will consist of discovery packages for litigation, privilege reviews, large volume FOIA/PA requests, subpoena responses, or records preservation requests.
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Other (specify):	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Information may be contained within reports to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, and resource requests.

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 website⁷ and described in the relevant Systems of Records Notices.

In instances where a prosecution occurs, defendants are afforded access to information in this system about them pursuant to the Federal Rules of Criminal and Civil Discovery.⁸

Disagreements regarding the context of information would be addressed during pre-trial or trial proceedings.

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).

<input checked="" type="checkbox"/>	<p>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):</p> <p>Litigation Support System – LSS – JCAM ID 1606 - ATO valid until 12/05/2024.</p> <p>Custom Database Application System – CDAS – JCAM ID 1605 – ATO valid until 10/11/24</p> <p>Litigation Automated Workflow System – LAWS – JCAM ID 2540 – ATO is carried under CDAS</p> <p>If an ATO has not been completed, but is underway, provide status or expected completion date:</p> <p>Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and JCAM milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes, are recorded in the Justice Management Division JCAM records. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer. As a matter of security policy, the Division does not release information regarding the existence of POAMs to the public.</p>
<input type="checkbox"/>	<p>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:</p>
<input checked="" type="checkbox"/>	<p>This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification,</p>

⁷ See <https://www.justice.gov/criminal/crm-freedom-information-act>

⁸ For more information on the Federal Rules of Criminal Discovery, see <https://www.federalrulesofcriminalprocedure.org/>. For more information on the Federal Rules of Civil Discovery, see <https://www.federalrulesofcivilprocedure.org/>.

	which may be detailed in the system security and privacy plan: The highest risk information contained in HUIS is related to investigative referrals and is considered a moderate risk in accordance with FIPS 199 and includes appropriate security controls for this categorization, and the sensitivity of the information.
<input checked="" type="checkbox"/>	<p>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</p> <p>LSS undergoes continuous assessments, penetration tests, and vulnerability scans, and is monitored through the CRM IT Security Continuous Monitoring Program. CRM performs vulnerability and configuration management scanning using both tools provided by the DOJ Office of the Chief Information Officer and provided by CRM IT. Continuous monitoring includes the security assessment process and a manual review audit occurs at regular intervals, to the extent required by the National Institute of Standards and Technology (NIST) special publication (SP) 800-53, Revision 4.⁹</p> <p>Incorporated cloud service providers, referenced in the appendix, are responsible for securing and enforcing identified security controls and informing the DOJ of any incidents.</p>
<input checked="" type="checkbox"/>	<p>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</p> <p>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 by JMD. Access to these logs is provided to the Justice Security Operations Center, who provided security analysis and log monitoring for unusual activity to the extent required by NIST SP 800-53, Revision 4.</p> <p>Information Owners and 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), may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the information owner.</p>
<input checked="" type="checkbox"/>	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.
<input checked="" type="checkbox"/>	<p>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:</p> <p>One-on-one and case-specific training, specific to this system, is conducted for newly authorized users, including contractors. ALS has designed and offers trainings to end-users</p>

⁹ See <https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22>.

on various aspects of the system. These trainings are either on demand or custom designed for specific projects.
--

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 Personal Identity Verification (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 [DAA-0060-2021-0001: Litigation Case Files](#) which determines the retention schedule based on the nature of the investigation.

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: Information Access and Protection Records](#) 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 JCAM 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 embedded 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.

Addendum

ALS Tool Inventory

Litigation Automated Workflow System (LAWS)

LAWS is a custom designed application of the Division's Custom Database Application System (CDAS).¹⁰ ALS uses LAWS to manage the workflow and track the progress of each case and their related requests. LAWS contains a front-end interface where the end-users can request the necessary access controls, data processing, case organizations, specific training requests, organizational meetings, technical assistance and other forms of request processing to ALS. ALS then routes the requests to the appropriate internal specialists to perform the needed actions and the requests are passed to other specialists if needed until the request is complete. LAWS also tracks which tools are used to process data. Both the end users and ALS personnel can perform live tracking of their individual requests.

Relativity

Relativity¹¹ is the Division's primary eDiscovery management tool. The Division employs a Customizable-off-the-shelf (COTS)¹² version of Relativity that allows ALS to maintain control and security over the tool. In the majority of cases, data is converted to a Relativity format and the processing, such as tagging, reviewing, redacting, batching and producing packages for release to the appropriate entities is conducted using Relativity. Within Relativity, ALS uploads the case documents and organizes the case at the direction of the end-users and performs administrative management of the individual cases. The end users then access the case data and perform the necessary reviews, analysis, redactions and grouping for release.

Systran

Systran¹³ is the Division's primary computer translation tool. Systran allows linguistic translation of individual documents or mass translation of documents within Relativity. It also has language identification capabilities and stores translations within the Relativity workspace. It is a COTS product that is available through Relativity.

Blackout

Blackout¹⁴ is the Division's primary native redaction tool. It is a COTS product that is available through Relativity as an enhancement. Blackout allows users to redact native documents such as Excels and Adobe PDFs directly from Relativity.¹⁵

Nuix Workstation

¹⁰ A PIA for the CDAS Environment is currently being developed.

¹¹ <https://www.relativity.com/data-solutions/ediscovery/>

¹² Although Relativity, its add-ons and the other tools listed below as COTS tools are often available as Cloud or Software-as-a-service (SaaS) tools, it is specifically procured and managed as COTS tools by ALS in order to maintain the isolation of LSS.

¹³ <https://www.relativity.com/data-solutions/customizations/app-hub/systran-software-inc/>

¹⁴ <https://www.relativity.com/data-solutions/customizations/app-hub/blackout/>

¹⁵ Without Blackout, redactions within Relativity are applied to an image file, instead of the native file.

Nuix Workstation¹⁶ is the Division's primary eDiscovery processing tool. It is a COTS product from Nuix to conduct a consistent, repeatable and forensically defensible indexing process across large volumes of source data to determine how to best process source documents or items. It is used to reduce the volume of electronically stored information (ESI) and convert it, if necessary, to forms more suitable for review and analysis when ultimately loaded in the Division's primary eDiscovery management tool, Relativity.

Nuix Investigate

Nuix Investigate¹⁷ enhances the capabilities of Nuix Workstation. It is a COTS product from Nuix that allows users to perform early case assessment (ECA) on ESI processed through Nuix Workstation. ECA can include identifying key facts and patterns within the data, identify relevance and privilege issues, uncover crucial information, spot notable case trends, speed up and enhance the legal decision-making process, and save legal costs.

Rampiva

Rampiva¹⁸ is a workflow automation software that interacts directly with Nuix Workstation. It is a COTS product that contains an in-built queuing system, which gives users the ability to automatically queue up processing jobs in Nuix Workstation. Multiple cases are staged and lined up to be fed into Nuix to automatically start processing as the previous job completes or fails. Additionally, this allows Nuix to continue processing outside of normal work hours without human supervision.

LAW PreDiscovery

LAW PreDiscovery¹⁹ is an additional eDiscovery processing tool that the Division employs. It is a COTS product from CloudNine that converts ESI into forms more suitable for review and analysis to be loaded in the Division's primary eDiscovery management tool, Relativity.

Nexidia

Nexidia²⁰ is COTS product that allows for phonetic searching of audio and video data. In a manner similar to Relativity's search, tagging and identification of relevant documents, Nexidia searches, tags and marks pertinent portions of audio data. To do this, Nexidia indexes audio based on phonemes, the smallest unit of human speech. Nexidia can identify individual speakers, handle multiple languages, dialects and accents.

Trial Director

Trial Director²¹ is the Division's primary transcript and trial presentation tool. It is a COTS product from IPro that allows users to manage transcripts, videos, and other evidence and organize exhibits in smart witness or trial workbooks. Additionally, it allows users to create video clips, deliver witness binders and exhibit lists, and issue condensed transcripts.

¹⁶ <https://www.nuix.com/technology/nuix-workstation>

¹⁷ <https://www.nuix.com/technology/nuix-investigate>

¹⁸ <https://rampiva.com/>

¹⁹ <https://cloudnine.com/software-training/law-prediscovery/>

²⁰ <https://www.nice.com/products/interaction-analytics/nexidia-legal-solutions>

²¹ <https://ipro.com/products/trialdirector/>

FolderSizes²² is a COTS product. It is a network-enabled disk space analyzer and folder size reporting tool for Windows. Additionally, it can search for files and folders by age, name, attributes, size, or owner. It can isolate largest files, oldest files, duplicate files, and temporary files. Finally, it generates reports for file types, attributes, owners, sizes, names, dates, and depths

AccessData FTK imager is a COTS product used by ALS to mount forensic computer images generated by Forensic Toolkit (FTK).²³ ALS uses this when they receive forensic images from one of the many computer forensic labs operating under the Department or under other law enforcement authorities. AccessData FTK imager allows ALS to mount the images to review the contents in order to determine which tool should process it. Additionally, it allows the extraction of original forensic images from multi-level forensic images which is a common practice in the processing of certain computer forensic labs.

Cellebrite Reader²⁴ is a COTS product used by ALS to open forensic images of cell phone data processed by Cellebrite.²⁵ Cellebrite Reader allows ALS to open and view the contents of a Cellebrite forensic report in order to determine how to best process it. Cellebrite is another forensic tool that is used by various computer forensic labs.

DatQC is a custom-designed fully insular self-enclosed desk-top utility that does not store information. DatQC performs quality control reviews on structured load or indexed files. It verifies the data integrity within the index, ensures that the data, the columns, their names, and internal data within are correct. It then allows quality control-based corrections.

LSU is a custom-designed fully insular self-enclosed desk-top utility that does not store information. LSU performs copy operations from one media into Division systems in a manner that ensures consistent copying and retains the integrity of the source data. LSU can also export PDF images and split them into separate images suitable for Relativity review.

Automated Litigation Support Automation (ALSA) is a custom-designed platform developed by the ALS team. ALSA is a SQL Server based system that routes projects and project information to the appropriate ALS processing system. ALSA orchestrates automation by communicating directly and orchestrating the project lifecycle within LAWS, Raptiva, Nuix and Relativity. Thus, it streamlines the processing of requests received from the case team by automating intake, processing, culling, imaging, text extraction through optical character recognition, publishing to Relativity, and production of case data. ALSA autonomously initiates, plans, executes, monitors, controls, and closes ALS activities

²² <https://www.foldersizes.com/>

²³ <https://www.exterro.com/forensic-toolkit> Forensic Toolkit is a forensic tool used to create forensic images of drives, disks, and files for both computer and mobile devices. This tool can acquire data from various sources, such as physical devices, logical drives and files, remote memory, and volatile data.

²⁴ <https://cellebrite.com/en/reader/>

²⁵ <https://cellebrite.com/en/home/>

CDS Convert²⁶ is a FedRAMP²⁷ approved, Cloud-based service provided by Complete Discovery Source (CDS)²⁸ who provides a broad range of electronic discovery and electronic forensic solutions for government agencies, law firms and corporations. CDS Convert leverages the Relativity²⁹ suite of discovery management software and applies proprietary feature enhancements to convert complex data formats which would otherwise require laborious custom workflows or secondary platforms to conduct a review. These formats include but are not limited to those used in mobile phones and tablets, business and financial chat applications, social media messaging services and development and issue tracking platforms. These formats can include but are not limited to forensic extraction tools such as Magnet Axium³⁰ or Cellebrite UDFR³¹ forensic image files.³² CDS maintains a research department to continuously develop solutions to apply to newly developed or updated formats as they emerge with evolving technologies. By converting these varied formats into the Relativity Short Message Format (RSMF), they can be processed using the Division's existing Relativity interface and displayed in the Relativity Short Message Viewer while preserving the Relativity Production, Analytics and Assisted Review and Review capabilities.

Transmission will be performed through the Justice Enterprise File Sharing System (JEFS), owned by the Justice Management Division (JMD), and administered by the Division. CDS Convert will use JEFS in a manner consistent with the previously published Departmental JEFS PIA.³³ The Department utilizes JEFS as a transport infrastructure only, and the Department has not designated JEFS as an official record-keeping system, a document archival system, or a document backup system.

As an addition to the Division's Privacy Risk Mitigation Strategy, CDS will not store or retain the information processed on behalf of the Division. The information processed is returned to the Division to perform their own discovery processing through Relativity. While processing a request, CDS will identify and track the request by the LAWS ID number assigned by ALS instead of case names, which could reveal PII. CDS employs a combination of both automated and manual controls to log all transactions that are taking place with Division data. Manual controls are customized in coordination with the Division to ensure compliance with the Division's audit needs.

Delegate³⁴ is a COTS which allows for the automation of tasks within Relativity such as the scheduling and execution of index builds, structured analytics, and concept clustering on daily basis after business hours.

²⁶ [CDS Convert - Complete Discovery Source \(cdslegal.com\)](https://www.cdslegal.com/)

²⁷ [Learn What FedRAMP is All About | FedRAMP | FedRAMP.gov](https://www.fedramp.gov/)

²⁸ [Federal Cloud Services - Complete Discovery Source \(cdslegal.com\)](https://www.cdslegal.com/)

²⁹ [eDiscovery & Legal Search Software Solutions | Relativity](https://www.relativity.com/)

³⁰ [Magnet Forensics](https://www.magnetforensics.com/)

³¹ [Cellebrite](https://www.cellebrite.com/)

³² Magnet Axium and Cellebrite UDFR are forensic processing tools that are used by various computer forensic laboratories. Forensic laboratories produce results in the form of a forensic image file or executable reports which are forensic copies and analysis of the data from the source data source. It is the forensic image and analysis that is produced in discovery packages. It is those images and reports that CDS Convert is converting into formats compatible with Relativity.

³³ https://www.justice.gov/d9/pages/attachments/2021/09/30/jefs_pia_final_draft_11-30-2017.pdf

³⁴ <https://relativity.com/relativity/assets/pdf/milyli-delegate-overview.pdf>

Chronicle³⁵ is a COTS product which ALS is looking to acquire for privilege logging in Relativity. By automating and simplifying the current process of managing privilege logs, Chronicle will enable users to allocate more time and resources to substantive legal work.

³⁵ <https://relativity.com/relativity/assets/pdf/milyli-chronicle-overview.pdf>