U.S. Department of Justice - JMD

Privacy Impact Assessment
for the
DOJ Mega 5 Evidence Management System

Issued by:
John E. Thompson
JMD Senior Component Official for Privacy

Approved by: Jay Sinha
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: January 26, 2026

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes:

- ***a) The information technology;***
- ***b) Its purpose;***
- ***c) How the information technology operates to achieve that purpose;***
- ***d) The general types of information involved;***
- ***e) How information may be used and shared, and;***
- ***f) Why a Privacy Impact Assessment was conducted.***

(Note: this section is an overview; the questions below elicit more detail.)

The DOJ Mega 5 Evidence Management System (EMS) is a cloud-based document management system (developed by Deloitte) used to provide a secure web-based application that enables U.S. Department of Justice litigation components to ingest, process, search, analyze, review, and produce electronic files and other data that have been collected in the course of Department litigation or investigations, or collected to aid in responding to other types of document/information requests, such as Freedom of Information Act (FOIA) requests or Privacy Act requests. EMS is utilized by DOJ litigation teams on a case-by-case-or as-needed basis depending on the size, scope, and complexity of the matter. Unique collections are created for each separate matter or use, and access rights are uniquely set and managed for each collection. Various types of information in identifiable form may potentially be part of gathered evidence maintained in the system used to support the Department litigation and investigation mission requirements.

The EMS achieves its purpose by using Relativity, which indexes electronic information uploaded into the system for attorneys, contractors, and staff to review. At its core, the system contains an indexed Structured Query Language (SQL) database, which maintains "meta" information. In eDiscovery this means information about the file such as creation dates, authors, email distributions, and similar. Relativity also uses web servers for data presentation and distribution, full text document search servers and indexers, concept clusters, analysis servers and indexers, as well as imaging servers and processors. These functions are combined in a web browser interface to give components a single cohesive tool in which to perform document review. These components are all part of the Relativity software package.

The information maintained in EMS may be accessed by DOJ authorized and cleared federal employees and contractors, but only after they have been given individualized permission to access a certain case and/or data in EMS. Privileged accounts require multiple levels of approval from authorized DOJ officials. System access is only granted to those persons who have a demonstrated need to have access to information maintained by the system. User access is limited to only information necessary to perform his or her work function. EMS users are required to sign DOJ Rules of Behavior and Computer Use Agreements. Training is also required for system administrator access. Account activity is monitored through triggered alerts, which are sent via Splunk to the Deloitte security team. Information maintained within EMS is disclosed or shared on a need-to-know basis and only as permitted by court orders, rules, or law.

System Administration accounts are reviewed quarterly to validate accounts are still necessary. Only SQL administrators and Domain administrators have access to DOJ data. Currently, there are four (4)

people with this type of access.

In accordance with Section 208 of the E-Government Act of 2002, JMD prepared this Privacy Impact Assessment because EMS will collect, use, and maintain information in identifiable form about members of the public.

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.

The DOJ litigating components are responsible for representing the United States Government in most domestic and foreign courts, and before grand juries and administrative or adjudicative bodies. To carry out this work, DOJ litigating components must ingest, search, analyze, and produce large amounts of data relevant to support DOJ litigation, discovery, or disclosure of document requests, as mandated by law and DOJ policy. The EMS application may be used by DOJ litigating components to support these efforts.

In addition, EMS allows for visualization tools to be used in the analyzing of data within the case file. EMS assists attorneys, paralegals, and other DOJ staff or contractors in reviewing investigation, litigation, and disclosure records about a specific case and provides a central workspace to bring case strategy and discovery together. Such activities include reviewing documents for relevance and privilege claims; tracking use of documentary evidence in litigation; preparing witness kits/binders for depositions, hearings, or trials; determining and organizing the facts about the case; and selecting exhibits for trial. EMS may also be used to help review and compile responses to other types of document requests, such as FOIA requests.

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
x	Statute	5 U.S.C § 301 28 U.S.C. §§ 514-19 28 U.S.C. § 534
	Executive Order	
x	Federal Regulation	28 C.F.R. Chapter 1
	Agreement, memorandum of understanding, or other documented arrangement	

x	Other (summarize and provide copy of relevant portion)	Federal Rules of Civil Procedure Federal Rules of Criminal Procedure Federal Rules of Evidence Federal Rules of Appellate Procedure Justice Manual

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.

(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
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	See Section 1 Exec. Summary. All information categories may apply to this system as any of the PII of the people identified in column #3 may potentially be collected as part of the litigation discovery or investigative process.
Date of birth or age	X	A, B, C and D	See comment above.
Place of birth	X	A, B, C and D	See comment above.
Sex	X	A, B, C and D	See comment above.
Race, ethnicity or citizenship	X	A, B, C and D	See comment above.
Religion	X	A, B, C and D	See comment above.

(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
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	See comment above.
Tax Identification Number (TIN)	X	A, B, C and D	See comment above.
Driver's license	X	A, B, C and D	See comment above.
Alien registration number	X	A, B, C and D	See comment above.
Passport number	X	A, B, C and D	See comment above.
Mother's maiden name	X	A, B, C and D	See comment above.
Vehicle identifiers	X	A, B, C and D	See comment above.
Personal mailing address	X	A, B, C and D	See comment above.
Personal e-mail address	X	A, B, C and D	See comment above.
Personal phone number	X	A, B, C and D	See comment above.
Medical records number	X	A, B, C and D	See comment above.
Medical notes or other medical or health information	X	A, B, C and D	See comment above.
Financial account information	X	A, B, C and D	See comment above.
Applicant information	X	A, B, C and D	See comment above.
Education records	X	A, B, C and D	See comment above.
Military status or other information	X	A, B, C and D	See comment above.
Employment status, history, or similar information	X	A, B, C and D	See comment above.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	See comment above.
Certificates	X	A, B, C and D	See comment above.
Legal documents	X	A, B, C and D	See comment above.
Device identifiers, e.g., mobile devices	X	A, B, C and D	See comment above.
Web uniform resource locator(s)	X	A, B, C and D	See comment above.
Foreign activities	X	A, B, C and D	See comment above.

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	See comment above.
Juvenile criminal records information	X	A, B, C and D	See comment above.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	See comment above.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	See comment above.
Grand jury information	X	A, B, C and D	See comment above.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	See comment above.
Procurement/contracting records	X	A, B, C and D	See comment above.
Proprietary or business information	X	A, B, C and D	See comment above.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	See comment above.
Biometric data:	X	A, B, C and D	See comment above.
- **Photographs or photographic identifiers**	X	A, B, C and D	See comment above.
- **Video containing biometric data**	X	A, B, C and D	See comment above.
- **Fingerprints**	X	A, B, C and D	See comment above.
- **Palm prints**	X	A, B, C and D	See comment above.
- **Iris image**	X	A, B, C and D	See comment above.
- **Dental profile**	X	A, B, C and D	See comment above.
- **Voice recording/signatures**	X	A, B, C and D	See comment above.
- **Scars, marks, tattoos**	X	A, B, C and D	See comment above.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	See comment above.
- **DNA profiles**	X	A, B, C and D	See comment above.

(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
- **Other (specify)**	X	A, B, C and D	Given the purpose of EMS, any biometric data relevant and necessary to litigation, investigations, and disclosure activities could be maintained in this system, including those not otherwise within the above- referenced categories. There is no classified information stored within the EMS environment. EMS cannot support processing classified content.
System admin/audit data:	X	A	System maintains system logs and other audit data on system and user activity
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**	X	A	
- **Date/time of access**	X	A	
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, and D	Given the purpose of EMS, any PII relevant and necessary to litigation, investigations, and disclosure activities could be maintained in this system, including PII not otherwise within the above- referenced categories, such as social media content.

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

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify): Documents may be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including directly from the individual about whom the information pertains.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Documents may be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including other government sources.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Documents may be obtained during investigation, litigation, discovery, or disclosure processes utilizing a variety of sources, including non-government sources.					

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	X		X	Within the EMS there are specific user roles (groups) defined which provide varying levels of access to data stored in the EMS. Critical functions are divided among different individuals based on their security group assignment and/or the role they play on a matter. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.
DOJ Components	X		X	DOJ components may share case information within EMS and collaborate with other DOJ components on a case-by-case basis, as needed and authorized by the DOJ Lead Case Attorney for that matter. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.

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	X			The agency may share case information within EMS and collaborate with other federal entities on a case-by-case basis, as needed and authorized by DOJ. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.
State, local, tribal gov't entities	X			The agency may share case information within EMS and collaborate with state, local, and tribal government entities on a case-by-case basis, as needed and authorized by DOJ. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			The agency may share data within EMS with opposing counsel or other persons or parties involved in litigation based on a need-to-know basis and for litigation purposes. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.

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.**
Private sector	X			Contractors to DOJ, opposing counsel involved in litigation and investigations, and private counsel who may handle certain litigation for the Department. Users will be allowed to modify data content for cases to which they are assigned. Component users are granted read, write, and delete access only on written authority of lead DOJ attorney working on the case, who may elect to do so for their internal support needs or upon issuance of a court order or mutual agreement between opposing parties.
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.

The information will not be released to the public for open data purposes.

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.

EMS contains information about individuals contained in documents collected from various parties in the course of litigation. Such documents include information DOJ components have collected about individuals pursuant to court order, warrant, subpoena, discovery request, or other lawful processes as part of authorized law enforcement or national security activities. But such documents also include

any information from any source that is part of the litigation matter being litigated by DOJ.

Distinguishing between the matters being litigated by DOJ, from the process of the litigation itself, the processes for the information collections as part of the matters being litigated are not relevant here.

Regarding the notices related to uses of this system to collect, use, or share PII for the DOJ processes of the litigation itself, to the extent individualized notice of such information processing is required by law, court rules, or DOJ policy, the Department and/or litigating components provide it; though they do not use this system to do so. Opposing counsel or the court may also provide individualized notice, depending on the circumstances. The Department, however, is not required to provide individualized notice to everyone whose PII may be implicated.

All EMS systems require a banner that users see before authenticating into the system. The banner verbiage is as follows:

This Deloitte Computer System is operated in the interests of various U.S. Government agencies, including the U.S. Department of Defense. This system, and all related equipment, networks, and network devices (specifically including Internet access) that store, process, transmit or display U.S. Govt. information are provided only for authorized use for Deloitte and U.S. Govt. interests., all system portions may be monitored for all lawful purposes, including ensuring authorized use, for system management, to facilitate protection against unauthorized access, to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized Deloitte or U.S. Govt. entities to test or verify system security. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed, or sent over this system may be monitored. System use, authorized or unauthorized, constitutes consent to monitoring of this system. Communications using, or data stored on, this system are not private. They are subject to routine monitoring, interception, search, and may be disclosed for Deloitte or U.S. Govt. authorized purposes. Unauthorized use subjects you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action.

The Department also publishes in the Federal Register generalized notice about maintenance of these records in the form of the Department's system of Records notices (SORNs). The applicable SORNs include:

- Justice/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and amended at 86 Fed. Reg. 37188 (July 14, 2021)

- 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. (May 25, 2017)

The records created, compiled, and maintained in this system to accomplish the Department's investigations, litigation, and discovery functions, may also be covered by the Department's litigation and general leadership case file SORNs, including:

- FBI/FBI-002, The FBI Central Records System, last published in full at 63 FR 8659, 671 (Feb 20, 1998), and amended at 82 FR 24147 (May 25, 2017)

- 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)

- JUSTICE/ATR-001, Antitrust Division Expert Witness File, last published in full at 54 Fed. Reg. 42060, 061 (Oct. 13, 1989), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files, last published in full at 72 Fed. Reg. 33515, 529 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 165 (May 25, 2017)

- JUSTICE/OIG-001, Office of the Inspector General Investigative Records, last published in full at 72 Fed. Reg. 36725 (July 5, 2007), and amended at 82 Fed. Reg. 24151, 160 (May 25, 2017)

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.

Given the investigation, litigation, and disclosure equities of the Department, other than as users of the system, individuals will generally not be provided an opportunity to voluntarily participate in the collection, use, or dissemination of information accessible within EMS.

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.

Individuals may follow the procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations. The records maintained in EMS, however, may be subject to certain exemptions to the access and amendment procedures, as articulated in the applicable SORNs, and in Subpart E, Part 16, Title 28, Code of Federal Regulations.

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):** 11/05/2024 (3-year ATO that expires on 11/5/2027) **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:** There are no privacy related items in the POA&M**.**
	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:
	This information or information 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 NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: After reviewing the information and use case for this system we determined that this system requires a FISMA Moderate designation due to the nature of the information it processes and the potential impact of a security event. The system handles sensitive but unclassified data, where a loss of confidentiality, integrity, or availability could have a serious—though not catastrophic—adverse effect on organizational operations, assets, or individuals. Key factors in this determination include: The absence of classified or national security information. The presence of business-critical data, where compromises could disrupt operations but are unlikely to lead to severe or irrecoverable damage.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The provider of EMS, Deloitte, is responsible for securing and enforcing identified security controls and informing the Department of any incidents. EMS is fully managed completely within the Deloitte ecosystem and only by Deloitte cleared staff pursuant to standards set via contract with DOJ. Deloitte's Federal Cyber Security Team has put in place several controls that control the use of sensitive information by all Deloitte staff and all users of the EMS system. These include:

	• Employee Rules of Behavior and Computer Use Agreements. • Assignment of unique account name and complex password. • Multifactor authentication and automatic enforcement of login via Windows Active Directory. Personal identity verification (PIV) cards are used for second factor authentication. • Access provided strictly based on approved authorizations. • Regular account reviews and removal of inactive accounts. Reviews include Monthly Audit of inactive users (no activity in 30 days) and disabling of login after 30 days of inactivity. • Access is provided at the level needed to perform business tasks. Additional permissions are not granted unless there is a demonstrated business need. • Annual Privacy and Information Security Training required for all users. • CCTV at multiple egress and ingress points at data centers. • 24/7 manned security at data centers. • Biometric Scanners at entrance to data center floors. • Proximity cards required to access federal racks at data centers. • Logical separations between zones. • Data encrypted using FIPS-140-2 compliant encryption technologies. using FIPS-140-2 compliant encryption. 2) The EMS system goes through the FedRAMP audit continuous monitoring cycles annually. Separate controls are tested annually in addition to the baseline controls. A SAR is created and shared with DOJ security team. At the end of the 3-year cycle, a new ATO is issued. In addition, the EMS system is documented in DOJ JCAM. The Deloitte ISSM is required by contract to work with JMD to maintain FISMA compliance and adhere to internal DOJ security standards in addition to any other requests that come up during normal operations.
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:** Within the EMS, specific user roles (groups) are defined in a way which provides varying levels of access to data stored in the EMS. Critical functions are divided among different individuals based on their security group assignment and/or the role they play on a matter. Generally, users will be allowed to access only information for cases to which they are assigned. Auditing functionality exists within the EMS to allow for specific user actions to be recorded in an audit log and backed up for a specified period. Information stored includes type of audit event, date and time audit event occurred, User ID, command used to initiate the audit event, success or failure of audit event and event result. All audited transactions within the EMS are written to a separate audit log table within the EMS database. The electronic audit log is protected from viewing by unauthorized users. Audit logs are captured through Splunk agents. Splunk is configured to flag certain events which are highlighted in the Security Operations Center (SOC) consoles. The SOC is in Rosslyn, VA, and is staffed 12 hours a day, five days a week. The GPS SOC analysts review the triggered events to determine if action is required. All logs are kept for 90 days to ensure previous events can be researched as required. The SOC is trained in identifying flags within the security information and event management (SIEM) tool and acts on those based on standard

	operating procedures. DOJ works with Deloitte to determine auditing requirements, and Deloitte shares audit data with DOJ upon request.
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**, including DOJ PGD 15-03, which specifically requires any information system which holds or processes DOJ information to adhere to DOJ and other associated Federal requirements.
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:** Personnel that have access to the system will take security training annually. Specifically, agency-specific training about safeguarding PII is provided to all employees and contractors of the agency. In addition, contract staff are required to take annual training on security and privacy conducted by their company. There is no other system specific training is provided.

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?

The information maintained in EMS may be accessed by authorized federal employees and contractors, but only after they have been given individualized permission to access a certain case and/or data in EMS. For government and other non-Deloitte users the process starts with an email from the DOJ Attorney who has been designated as the primary client for this engagement sending an email requesting access to a list of users. The request will also indicate if the users can see all or some documents/information and what reason they have for access. For Deloitte Users the access is requested by the Deloitte Project Manager. EMS is fully managed completely within the Deloitte ecosystem and by Deloitte cleared staff. Software or hardware partners do not have access. Within EMS, specific users' roles (groups) are defined in a way which provide varying levels of access to data stored in the EMS. Critical functions are divided among different individuals based on their security group assignment and/or the role they play on a matter. Generally, users will be allowed to view only information for cases to which they are assigned. Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Audit Logs are shared as requested. Deloitte provides DOJ updates on outstanding POAM items. Deloitte will work with DOJ to discuss what audit logs should be shared, and what should be provided in executive rollups.

Please note: Individual case files can be locked down at the folder level based on JMD or DOJ component requests. Deloitte does not lock down folders unless specifically identified by DOJ engagement team.

The following controls manage access to and the use of sensitive information. This includes Deloitte collecting, executing and managing the following access controls:

- Employee Rules of Behavior and Computer Use Agreements

- Assignment of unique account name and complex password
- Multifactor authentication and automatic enforcement of login via Windows Active Directory. PIV/CAC cards are used for second factor authentication
- Access provided strictly based on approved authorizations
- Regular account reviews and removal of inactive accounts. Reviews include Monthly Audit of inactive users (no activity in 30 days) and disabling of login after 30 days of inactivity
- Access is provided at the level needed to perform business tasks. Additional permissions are not granted unless there is a demonstrated business need
- Annual Privacy and Information Security Training for all users
- CCTV at multiple egress and ingress points at datacenters
- 24/7 manned security
- Biometric Scanners at entrance to data center floors
- Proximity cards required to access federal racks
- Logical separations between zones
- Data encrypted using FIPS-140-2 compliant encryption technologies

3) Administrative Controls
    - Access is provided to end users ONLY if approved by DOJ.
    - Workspace permissions can be locked down. DOJ determines access to individual cases or files and will request Deloitte to lock down specific files to specific people.
    - Logging on all files is implemented within each workspace.

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.)

Data will be retained in the system until the materials no longer need to be stored on the system, typically after an investigation or case has closed or settled, and the information is not needed for other cases or investigations and in line with the NARA record retention schedule DAA0060-2017-0007 (Records Documenting Compliance with Preservation Obligations for Component Information) which requires data to be destroyed within 3 years after preservation obligation ends. Data custodians within components will be tasked with reviewing the audit trail to determine when and which data can be destroyed. Since DOJ is the steward of the data; DOJ will be responsible for noting when the 3-year clock starts to run on the data within the system. The Deloitte Project Manager overseeing the case is responsible for timely coordinating this activity with the lead DOJ Attorney. Deloitte will not remove any data automatically regardless of NARA standards unless approved by DOJ Attorneys and lead DOJ business leaders.

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. X 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:

- Justice/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec. 30, 1999) and amended at 86 Fed. Reg. 37188 (July 14, 2021) (https://www.justice.gov/opcl/doj-systems-records#DOJ).

  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. (May 25, 2017) (https://www.justice.gov/opcl/doj-systems-records#CIV).

The records created, compiled, and maintained in this system to accomplish the Department's, litigation, and discovery functions, may also be covered by the Department's litigation and general leadership case file SORNs, including:

- 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)

- JUSTICE/ATR-001, Antitrust Division Expert Witness File, last published in full at 54 Fed. Reg. 42060, 061 (Oct. 13, 1989), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/CIV-001, Civil Division Case File System, last published in full at 63 Fed. Reg. 8659, 665 (Feb. 20, 1998), and amended at 82 Fed. Reg. 24147 (May 25, 2017)

- JUSTICE/USM-013, U.S. Marshals Service Administrative Proceedings, Claims and Civil Litigation Files, last published in full at 72 Fed. Reg. 33515, 529 (June 18, 2007), and amended at 82 Fed. Reg. 24151, 165 (May 25, 2017)

- JUSTICE/OIG-001, Office of the Inspector General Investigative Records, last published in full at 72 Fed. Reg. 36725 (July 5, 2007), and amended at 82 Fed. Reg. 24151, 160 (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.***

As indicated in the table within section 3.1, every information category will potentially be stored within EMS given the nature of investigatory and litigation materials. The main potential privacy risks associated with this system and the data that is being stored and processed are: (1) unauthorized access, (2) unauthorized disclosure or breach of PII, and (3) data over-collection. To mitigate these risks, only cleared DOJ personnel and contractors as well as any other external users authorized by the DOJ attorney and that have a need-to-know, will have access to this system; and all users must use two-factor authentication (PIV card and PIN). Litigating components must document their authority use of EMS in JCAM. JMD OCIO has set-up a special profile to catalogue such ATOs. JMD owns the system from an AO perspective and is responsible for issuing ATOs for each component use. System monitoring is a Deloitte-only function. DOJ is the steward of the data within EMS but monitoring, auditing, scanning are Deloitte specific tasks. To enforce need-to-know requirements, components will then have a separate instance created so they only have access to documents managed by their respective component. Separate instances are virtually separated as is the data associated with each workspace. To further mitigate privacy risks resulting from the sensitive information, including PII, maintained in EMS, JMD and Deloitte have implemented numerous security controls, consistent with Section 6, above. For instance, EMS is a Federal Risk and Authorization Management Program (FedRAMP) authorized software solution. The FedRAMP is a standardized security assessment and authorization process for cloud products and services used by U.S. federal agencies. As a result, EMS was reviewed by an authorized third-party assessment organization and authorized to operate by JMD's authorizing official.

Deloitte is required to submit a Security Impact Assessment and obtain approval from JMD prior to software acquisition and implementation. A DOJ authority-to-operate (ATO) has been granted as an assessment and documentation of NIST Special Publication 800-53 security and privacy controls have been implemented. To further safeguard information maintained in EMS, all data at rest, including backups, are encrypted, and deemed to be FIPS 140-2 validated. Data in transit, which is both internal and external web traffic, is encrypted as well using Transport Layer Security (TLS) 1.2.[1]

The Information Security System Officer and system stakeholders will meet with the cloud service provider, Deloitte, periodically to perform continuous monitoring of security controls and any changes that may occur. Deloitte has incident response procedures that include preparation, detection and

[1] The "Transport Layer Security" protocol is used "to secure communications in a wide variety of online transactions . . . . Any network service that handles sensitive or valuable data, whether it is personally identifiable information (PII), financial data, or login information, needs to adequately protect that data." NIST, Special Publication 800-52, rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (Aug. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf. Department of Justice Privacy Impact Assessment JMD/DOJ EMS ensure that DOJ employees and contractors comply with this training.

analysis, containment, eradication, recovery, and collaboration/notification of DOJ. An annual system contingency plan and incident response tabletop exercise will be performed in accordance with NIST 800-53 rev. 5 continuous monitoring guidance.

To mitigate the risk of data over-collection, the users that are a part of the litigating components are trained to perform e-discovery in a manner that data collection is intended to identify information relevant to the purpose of the litigation matter at hand. By Department Order, all DOJ users (federal and contractor) with access to Department networks must complete annual Cybersecurity Awareness Training. In addition, Deloitte personnel complete the GPS Technology Center Attestation. The security courses include information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign an EMS Rules of Behavior agreement confirming that they have completed security training and that they agree to abide by such requirements reviewed in the courses. Failure to successfully complete this training can result in termination of the employee or contractor's access. Participation in the training is tracked to ensure that DOJ employees and contractors comply with this training.