United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
DOJ Learning Management System

Issued by:
Morton J. Posner
Senior Component Official for Privacy

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

Date approved: June 16. 2025

(May 2022 DOJ PIA Template)

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 the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The U.S. Department of Justice (DOJ) Learning Management System (LMS) is a commercial-off-the-shelf suite of SAP [1] SuccessFactors Human Capital Management (HCM) Talent Management applications. These applications support DOJ's efforts relative to Executive Order 13111, *Using Technology to Improve Training Opportunities for Federal Government Employees* (January 12, 1999); the President's Management Agenda (PMA) – Strategic Management of Human Capital, and the e-Government Human Resources Line of Business – Human Resource Development (HR LOB/HRD). The system is primarily governed by DOJ Human Resources Order 1200.1. Additional policy documents apply depending on specific use cases or component.

LMS manages web and classroom-based learning activities. The major functions of the system include providing access to commercial and component-specific web-based courseware, managing an on-line catalog of course offerings, automating training registration and approval processes, online individual development planning, online testing and surveys, tracking of training resources, management of and reporting on training data, and tracking of training completions.

LMS serves a large segment of DOJ, covering employees and contractors in all components except for the Federal Bureau of Investigation (FBI) and the Federal Bureau of Prisons (BOP). While all DOJ components, except for the FBI and BOP, have access to and can leverage LMS for their individual training needs, the following components have established their own separate iterations of LMS, within the LMS system boundary, and identify their learning environment by the following:

- Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) – Justice Talent Management System
- Drug Enforcement Agency (DEA) – DEA Learning System (DEALS)
- The United States Marshals Service – Learn United States Marshals Service (LearnUSMS)
- Executive Office of the United States (EOUSA), and all other divisions. – LearnDOJ

The system is also used to coordinate and/or deliver training to task force officers; as well as state, local, and international law enforcement and emergency response partners. Currently, only DOJ employees can access the LMS with a valid DOJ personal identity verification (PIV) Card[2]. Outside entities that require training are manually entered by an DOJ LMS Admin (for record keeping).

The system collects information on the training and development conducted or sponsored by DOJ

---

[1] https://www.sap.com/about/company.html
[2] A PIV card is a physical artifact (e.g., identity card, "smart" card) issued to an applicant by an issuer that contains stored identity markers or credentials (e.g., a photograph, cryptographic keys, digitized fingerprint representations) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). See https://csrc.nist.gov/glossary/term/piv_card.

components for their employees, contractors, and task force officers; as well as state, local, international law enforcement and emergency response partners. Records that contain information about individuals include those for learners, instructors, and administrators. For federal employee learners and instructors, this data includes names, work address, other information publicly available on federal employees (name and email address if used at all. No other PII is kept in the LMS), as well as Race and National Origin (RNO) on learners pursuant to Equal Employment Opportunity Commission (EEOC) Management Directive 715[3]. (RNO data is maintained in a privacy table not accessible to anyone through the application interface except for defined personnel/EEO staff.)

The system is used for authorized purposes and collects, maintains, uses, and disseminates information in identifiable form, for example, names, business and personal email addresses, and employment information. These examples are linked or linkable to individuals and are considered personally identifiable information (PII).

The program is managed by the Justice Management Division (JMD), Human Resources Staff, but DOJ contracts for the system through the Office of Personnel Management's USA Learning Program, a government shared service provider. The system runs on infrastructure provided by Amazon Web Services (AWS) Government Cloud (GovCloud) and is owned and operated by SAP National Security Services (NS2).

Pursuant to the privacy provisions of the E-Government Act of 2002 and the Office of Management and Budget's (OMB) implementing guidance (Memorandum-03-22), JMD is required to prepare a Privacy Impact Assessment (PIA) for this system. JMD's use of DOJ Learning Management System is covered by the Plateau Learning Management System PIA (May 2010) which requires update due to expansion of external users and changes in technology, data collected, and applicable authorities. This PIA will replace the Plateau Learning Management System PIA from 2010.

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.

LearnDOJ (SAP SuccessFactors) is the Department of Justice's (DOJ) enterprise-wide Learning Management System (LMS), replacing the legacy Baseline LMS, named Plateau. It is a web-based, Software-as-a-Service (SaaS) solution designed to deliver, manage, and track mandatory and professional development training for DOJ personnel and authorized users. The system enables DOJ Components to ensure training compliance, workforce development, and readiness across the enterprise.

At initial rollout, the following SAP SuccessFactors modules are in use:

---

[3] For more information on EEOC Management Directive 715 *see:* https://www.eeoc.gov/federal-sector/management-directive/instructions-federal-agencies-eeo-md-715.

- **Learning** (used across DOJ Components, excluding BOP and FBI),
- **Succession and Development**, and
- **Performance and Goals** (used by ATF only).

The Learning module delivers required and optional training content, while the other two modules support career development and performance management for select Components. ATF and Marshals are the only two DOJ components currently using the Succession and Performance modules. ATF is starting to sunset their modules may be implemented in future phases. Currently there are no new modules being considered for use in the future.

LearnDOJ collects and maintains PII, including employee and contractor names, work email addresses, component affiliations, and training history. This information is essential to assign courses, track completion status, and generate compliance reports for DOJ leadership and auditors.

The platform supports DOJ's mission by:

- Enabling compliance with training mandates under laws and policies such as the Federal Information Security Modernization Act (FISMA), OMB M-19-23, and DOJ-specific requirements;
- Supporting performance management, employee development, and organizational planning; and
- Providing audit trails and documentation necessary for internal and external oversight.

Although LearnDOJ is not used directly for criminal or civil law enforcement or intelligence activities, it plays a critical administrative role in maintaining a skilled, well-trained, and compliant workforce. The system's reporting and analytics functions may also be used to identify trends, training gaps, or areas of concern, allowing components to make informed decisions about workforce development and readiness.

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

Authority	Citation/Reference
Statute	44 U.S.C. § 3101, Records management by agency heads; general duties. Training information is collected and maintained under the provisions of the Government Employee Training Act (GETA), as codified in 5 U.S.C. §§ 4101-4118, with accompanying regulations promulgated in 5 C.F.R. § 410.311. FISMA, codified at 44 U.S.C. § 3541 et seq., requires federal agencies to provide annual cybersecurity awareness training (CSAT) for all users of federal information systems.

Executive Order	Executive Order 11348, as amended by Executive Order 12107 also provides general authority for the collection of training information.
Federal regulation	OMB Memorandum M-19-23
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	

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	First name, last name
Date of birth or age			
Place of birth			
Sex			
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A and B	ATF is the only component that collects the last four digits of the SSN.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			

(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
Personal e-mail address	X	B, C, and D	Personal e-mail is sometimes used for non-DOJ learners.
Personal phone number	X	B, C, and D	Personal phone number is sometimes used for non-DOJ learners.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records	X	A and B	Law Enforcement and US Attorneys use training for Qualification purposes.
Military status or other information			
Employment status, history, or similar information	X	A and B	User's employment status (e.g. full-time, part-time, intermittent)
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	A and B	Professional certifications and licenses. Completion Certs are created once the user completed the training.
Legal documents			
Device identifiers, e.g., mobile devices			Mobile is not yet implemented. If implemented, device identifiers will be collected.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			

(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
Proprietary or business information	X	C and D	Proprietary and business information can be included in presentations from vendors and guest speakers.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A and B	Training includes photo(s) of the speaker(s)
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			From a user perspective, there are no voice recordings captured training is delivered in a one-way format. However, from a course content perspective, some trainings do include pre-recorded audio from presenters that is embedded within the course materials.
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	Administrator log-in date/time information, for audit purposes User Account information and Date of completion
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**			
- **Queries run**			
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):			

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		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify): Users are able to enter and edit selected information in their user profile					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Information about users is collected from DOJ's Global (e-mail) Address List, payroll data from the National Finance Center (NFC), and payroll data from U.S. Department of the Treasury's Human Resources (HR) Connect. These three sources are used to populate user profiles of federal employees and contractors. Information on non-DOJ personnel who participate in training may be entered by LMS staff for record keeping purposes only.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Information on non-DOJ personnel who participate in training may be entered by LMS staff for record keeping purposes only.					

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	Component learning administrators may run reports on the learning activities of their component.

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.**
DOJ Components			X	JMD administrators may run reports on training participation to gauge compliance with mandatory training requirements.
Federal entities		X		Training reports for government employees are forwarded to OPM to comply with the requirements of their Enterprise Human Resources Integration program. Non-DOJ personnel who participate in and complete training may provide certificates of completion generated by the LMS.
State, local, tribal gov't entities	X			Non-DOJ personnel who participate in and complete training may provide certificates of completion generated by the LMS.
Public	X			Non-DOJ personnel who participate in and complete training may provide certificates of completion generated by the LMS.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			If required and related to the litigation.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

No information will be made 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.

The information is not directly collected from the individuals by the learning system. LMS collects this information from payroll information from NFC (for DOJ employees), Department of Treasury's HR Connect (for ATF employees), and DOJ's Meta-Directory (email) for contractors. Non-DOJ users' information is manually entered by a DOJ LMS Admin.

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.

The information in LMS is automatically collected from the NFC database or component equivalent (e.g., HR Connect for ATF) and DOJ's Meta-Directory. Individuals do not have an opportunity to decline to provide information. DOJ uses NFC for LMS file creation and deactivation. ATF uses HR Connect.

For ATF external learners, statements are included on ATF F 6400.1, Training Registration Request for Non-ATF Students and ATF F 6330.1, Application for National Firearms Examiner Academy indicating that disclosure of SSN is voluntary and identifying the effects of non-disclosure. Non-disclosure may result in denial of the request, or the applicant not being registered for the requested program. For ATF instructors, ATF Employee Instructor Application Form ATF F 6140.2 states that collection is voluntary, but that failure to disclose certain information may result in individuals not being eligible to serve as an instructor.

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.

For LearnDOJ and DEALS, all employees and contractors are automatically granted access to the LMS learner site upon creation of their records in the NFC (for federal employees), HR Connect (for ATF users) or the Global Address Locator (for contractors) databases. Using their DOJ credential, employees and contractors can see their scheduled, in process, and completed training and can generate certificates of completion for completed training. Administrator accounts are created on an as-needed basis and require submission of an additional signed Rules of Behavior (ROB) form. Component Training Coordinators submit

the signed ROBs to their Component Key System Administrators, who then forward them to the JMD Key System Administrator. Pursuant to the Privacy Act of 1974, individuals may request access to records pertaining to them, seek correction or amendment of inaccurate information, and receive notification of these procedures. Note: LMS PII fields are locked down. Users cannot update their information directly and must follow DOJ Privacy Act regulations outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations, for any changes. Users are notified of these procedures through system login banners, privacy documentation during onboarding, and applicable system policies and system of records notices.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** 10/13/2023-10/13/2026 **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 outstanding privacy-related POAMs for the LearnDOJ system at this time.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**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, which may be detailed in the system security and privacy plan:** The system is a shared service designed and built to provide service to U.S. Government agencies and the security requirements were developed and evaluated in accordance with The Federal Risk and Authorization Management Program, or FedRAMP. The system security controls were selected to comply with DoD Level 4 and FIPS 199 Moderate. The system security has been assessed by a Third-Party Assessment Organization ("3PAO") and has been issued Authority to Operate from The General Services Administration and The Defense Information Systems Agency.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify**: Ongoing monitoring and evaluation activities are

	conducted to safeguard information within the LearnDOJ system. These include routine security assessments, audit log reviews, vulnerability scanning, and annual control testing in accordance with DOJ and NIST requirements. Access to PII is role-based and monitored to prevent unauthorized use or disclosure.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The SAP NS2 Information System Security Engineer (ISSE) and Enterprise Monitoring Team utilize Splunk[4] with Enterprise Security to perform automated and near real-time review and analysis of audit records. Audit logs are continuously monitored, and suspicious activities are reviewed as they occur. Alerts are correlated, and tickets are opened promptly for further investigation and tracking. Splunk ingests logs from key sources including CloudWatch, CloudTrail, CMDB, and VPC Flow Logs. These tools are referenced in the SAP NS2 SSP to demonstrate the log review and monitoring process. However, they are not included in the IPA since they do not function as direct interfaces or interconnections through hypertext transfer protocol secure (HTTPS) Event Collector (HEC) and AWS Kinesis Data Streams. This continuous monitoring process ensures timely detection and response to security events across the LearnDOJ environment. Audit logs are generated and reviewed by SAP NS2 in accordance with their internal policies and FedRAMP requirements.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each Component is required to implement foundational privacy-related training for all Component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** There is no specific training for the Learning Management System.

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?

Data is extracted and disclosed based on the nature of the request. LMS data is securely transmitted using DOJ approved methods, including encryption in transit (HTTPS, secure file transfer). For all LMS processes, scripts developed by DOJ Office of the Chief Information Officer (OCIO) are used to process the data. Individual transcripts or learning records in electronic format are processed if the inquiry concerns a particular individual(s), or electronic spreadsheets of data are used for multiple individuals if the nature of the request is broader and is intended to address broader program requirements.

Possible risks are unauthorized access and/or misuse of data. Training-related information may be

[4] Splunk is covered by separate privacy documentation here: https://www.justice.gov/opcl/media/1363231/dl?inline.

subject to release under the Freedom of Information Act (FOIA), if requested and if it meets applicable FOIA disclosure criteria. Only the minimum amount of information needed to accomplish the purpose for which the information is collected. The information will only be shared with authorized users who have a legitimate need to know. All requests for training data from the Department are processed by a select group of LMS system administrators. These administrators ensure that only the minimum amount of data required to fulfill each request is extracted from the LMS and disclosed to the requesting party. Where possible, PII is masked or not included in the information being shared. LMS system administrators will only process requests for information received through the appropriate component program office or at the behest of the Assistant Director, Learning and Workforce Development, Human Resources Staff, Justice Management Division or component equivalent for the respective component domains. The potential risk for unauthorized disclosure/misuse is mitigated by:

- Limiting the number of authorized users and the data they may access;
- Providing initial and annual system security training; and
- Limiting physical access to the system hardware.

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.)

Law Enforcement Officer Training Records, DAA-0060-2017-0009-0001 (Delete 25 years after last action);

Legal, Investigative, and Litigation-Specific Training Records, DAA-0060-2017-0009-0002 (Destroy between 6 year(s) and 10 year(s) after last action);

Administration of Justice Technical Skills Training Records, DAA-0060-2017-0009-0003 (Destroy between 6 year(s) and 10 year(s) after cutoff (annually));

Training Administration Records, DAA-0060-2017-0009-0004 (Destroy 6 year(s) after cutoff (annually));

Ethics Training Records, DAA-GRS-2016- 0014-0002 (Destroy when 6 years old or when superseded, whichever is later, but longer retention is authorized if required for business use); and

Individual Employee Training Records, DAA-GRS-2016-0014-0003 (Destroy when superseded, 3 years old, or 1 year after separation, whichever comes first, but longer retention is authorized if required for 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. __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:***

System audit, access, and administration data are covered by Justice/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 FR 3718 (July 14, 2021), https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf.

OPM/GOVT-1, General Personnel Records (OPM's government-side SORN covering training records about federal employees (including contractors and volunteers)), 71 FR 35342 (June 19, 2006), https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.

ATF, DEA, and USMS have their own individual SORNs covering certain training records in their components:

ATF-010, Training and Professional Development Record System, 68 FR 3551, 3562 (Jan. 24, 2003), https://www.govinfo.gov/content/pkg/FR-2003-01-24/pdf/03-1576.pdf.

DEA-015, Training Files, 52 FR 47182, 217 (Dec. 11, 1987), https://www.justice.gov/opcl/docs/52fr47182.pdf.

USM-006, United States Marshals Service Training Files, 72 FR 33515, 522 (Jun. 18, 2007), https://www.govinfo.gov/content/pkg/FR-2007-06-18/pdf/E7-11543.pdf.

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.

LearnDOJ collects a limited amount of PII to support the Department's training and workforce development efforts. Like any system that manages user data, there are potential privacy risks such as unauthorized access, collecting more data than needed, keeping information longer than necessary, or sharing it inappropriately. The following measures are in place to help reduce those risks.

Access to LearnDOJ is limited based on user roles. The user role is only created to allow individuals to complete or request training for themselves. Only staff who need access to perform their job responsibilities can view or manage data in the system. Login requires PIV card authentication, and administrative access is granted following the principle of least privilege. Access rights are reviewed regularly.

All information sent to or from LearnDOJ is encrypted in transit and at rest. These protections meet DOJ and FedRAMP High standards, but the overall system authorization is officially approved at the FedRAMP Moderate level and is managed within the SAP NS2 environment, which hosts the platform.

The system keeps audit logs to track login activity and changes made by users with administrative access. LearnDOJ is hosted in a FedRAMP-authorized environment with strong physical security controls in place, including restricted access and environmental protections. DOJ personnel with system access complete annual privacy and security training. Administrators follow DOJ policies for acceptable use and handling of sensitive data.

The system only collects basic information needed to assign and track training—such as name, DOJ email address, component, and training history. It does not collect sensitive PII like full Social Security numbers (the system collects just the last four numbers of Social Security numbers) or birthdates. The information collected is the minimum required to meet DOJ's training and compliance needs.

Training records are kept according to DOJ records retention schedules. LearnDOJ is supported by SAP NS2 and GP Strategies, who provide technical and implementation services. These vendors are under contract and authorized to support DOJ systems. No data is shared outside DOJ or these approved vendors.

When users log into LearnDOJ, they see a system use notice that informs them their activity may be monitored, and that training data is being collected. DOJ policy also outlines appropriate use of IT systems and expectations for handling personal data.