United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for
DOJ Logging as a Service (Splunk)

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

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: November 11, 2022

(May 2019 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 Department of Justice (DOJ or "the Department") Logging as a Service (LaaS) platform comprises the DOJ Justice Management Division (JMD), Office of the Chief Information Officer (OCIO), Cybersecurity Services Staff (CSS) enterprise LaaS application. JMD LaaS currently utilizes software by Splunk Inc. to collect, store, query, and correlate machine logs. As a result of LaaS capturing these actions, the application can generate graphs, reports, and alerts in support of the Department's audit logging and monitoring. LaaS aims to make machine data accessible across an organization. The LaaS application identifies data patterns, provides metrics, diagnoses problems, and provides intelligence for business operations.

The type of information collected, maintained, used, or disseminated by LaaS is audit log data[1] that traverses the Department's networks. The information retrieved may include Personally Identifiable Information (PII).[2] The LaaS widget dashboards[3] may also identify system events (i.e., a potential incident) or insider threat inquiries, based on data from, and rules set for, DOJ security devices.[4] DOJ will then correlate, investigate, analyze, and remediate, these prioritized events.

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.

DOJ LaaS delivers a wide array of capabilities of the Splunk Enterprise platform, such as

---

1 Log Data refers to what type of event occurred; when the event occurred; where the event occurred; the source of the event; the outcome of the event; and the identity of any individuals or subjects associated with the event.
2 PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. See OMB Circular A-130, "Managing Information as a Strategic Resource" at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf.
3 Widget Dashboards is a term used by Splunk, allowing users to query ingested logs. A functionality that Splunk offers is the ability to visualize (tables, graphs) the data. Splunk dashboards are a way to save queries for repeated use and view. Custom dashboards are built for Splunk users to search and query for audit events of interest.
4 Security Devices refers to firewall, intrusion detection system, proxy, mail gateway, server operating system logs (e.g., Windows, UNIX, Linux), VPN, Blue Coat Proxy logs, Windows Desktop Security, and network devices (e.g., routers, switches).

searching, monitoring, dashboards, reporting, and analyzing mission essential real-time and historical machine data via a service centrally and uniformly delivered by the CSS LaaS Team. The CSS LaaS Team manages and updates the Splunk Enterprise platform uniformly, so all customers of the service receive the most current features and functionality. Splunk is utilized by all DOJ Components, except the Federal Bureau of Investigation (FBI). In addition, certain other Federal government agencies leverage DOJ's shared cybersecurity services, such as the Federal Retirement Thrift Investment Board (FRTIB), and Court Services and Offender Supervision Agency (CSOSA). These agency customers also may source information maintained on this system.

The DOJ CSS Splunk Enterprise platform captures, indexes, and correlates real-time and historical auditable events in a searchable repository from which it can generate graphs, reports, alerts, and dashboards in support of audit logging and monitoring for the Department. Splunk aims to make machine data accessible across an organization. It identifies data patterns, provides metrics, diagnoses problems, and provides intelligence for business operations. Splunk collects, normalizes, aggregates and indexes millions of events from thousands of assets across the network into a manageable stream that is prioritized according to risk, exposed vulnerabilities, and the criticality of the assets involved. These prioritized events can be correlated, investigated, analyzed, and remediated. Currently, Splunk receives, but is not limited to receiving, the following feeds from applications that forward data to Splunk: firewall, antivirus, Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), intrusion detection system, proxy, mail gateway, server operating system logs (Windows, Unix, Linux), Virtual Private Network (VPN), packet capture (NCA), Blue Coat Proxy logs, Windows Desktop Security, and router logs.

The purpose of Splunk is to index collected data from disparate security devices; normalize the data; provide JSOC analysts a "single pane of glass" to monitor security devices; provide Service Delivery Staff (SDS) administrators a tool to observe the health of the network; and to assist components with auditing requirements. The JMD Splunk environment is a distributed environment composed of multiple Splunk servers with dedicated functions that support Splunk's overall data ingestion and data query capabilities. Splunk indexers are the instances that ingest and house the data whereas Splunk search heads provide a user interface (UI) for users to query data. Splunk primarily receives logs through Splunk universal forwarders (lightweight endpoint agents) or intermediate heavy forwarders (full Splunk Enterprise instances). Data is collected by forwarders and routed to indexers where it is parsed and written to disk. Search heads connect to indexers and provides the ability to query data and create dashboards, alerts, and reports. All events are monitored by JSOC analysts.

Splunk collects, maintains, uses, and disseminates data that traverses the Department's networks. The information retrieved may include Personally Identifiable Information (PII). Splunk stores and disseminates via the Splunk widget dashboard data from security devices as well as rules that identify an event (potential incident) or Insider Threat Prevention & Detection Program (ITPDP) inquiry. Every class of user authorized to access Splunk goes through a Web UI. The CSS Splunk Support team, CSS Operations Support team, and CSS Engineering Support team are the only individuals who have access to the hardware and backend database. Component employees can request web accounts to Splunk with limited access restricted to events relevant

to their Component. Only the JSOC has access to all DOJ Component data.

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	**X**	Federal Information Security Modernization Act of 2014, Pub. L. 113- 283, 128 Stat 3073.
	Executive Order	**X**	Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)
	Federal Regulation		
	Agreement, memorandum of understanding, or other documented arrangement	**X**	Interagency Agreement (IAA) must be executed between DOJ and external federal agency subscribers which specifies the goods to be furnished or tasks to be accomplished by JMD OCIO CSS.
	Other (summarize and provide copy of relevant portion)	**X**	Office of Management and Budget (OMB) Circular No. A-130

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
Name	X	A and B	Names are required for Splunk account creation. Splunk accounts are created leveraging the user's name and email address.
Date of birth or age			
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address	X	A, B, C, D	Mail server logs are ingested into Splunk. Therefore, LaaS may maintain personal email addresses from anyone sending emails to or from DOJ.
Personal phone number			
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(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
Device identifiers, e.g., mobile devices	X	A	AirWatch logs (logs from mobile devices) may contain user identifying information such as name, organization, and phone number.
Web uniform resource locator(s)	X	A, B, C, D	Since the Splunk environment's primary objective is to support security review and investigations, there are security tools, and therefore logs, that contain URLs
Foreign activities	X	A, B, C, D	Depending on the security tool/application, Splunk could detect activity from non-DOJ/foreign devices
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			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			

(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
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A, B, C and D	Splunk collects relevant security logs[5] to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and /or data of access (e.g. Justice Privileged Access Management (JPAM) logs).
- **User ID**	X	A and B	Splunk collects IRP related logs.
- **User passwords/codes**	X	A and B	LaaS collects passwords for user accounts when federated authentication is not available. Otherwise user password is logged by a system outside of LaaS. The system may log those passwords, although that is not the intent.
- **IP address**	X	A, B, C and D	Splunk collects IRP related logs.
- **Date/time of access**	X	A, B, C and D	Splunk collects IRP related logs.
- **Queries run**	X	A and B	There are audit logs or search queries that would be captured per reviews of the system. Splunk audits queries run. Authorized users would be DOJ and other federal government personnel.
- **Content of files accessed/reviewed**			
- **Contents of files**			

[5] Security logs refers to the JMD OCIO and JSOC mandated logs that need to be collected from systems throughout the agency. These include Anti-Virus, DNS, DHCP, IDS, Web application, PowerShell and the logs contain date. See NIST 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations" control AU-02 "Event Logging" at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

(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 (please list the type of info and describe as completely as possible):	X	A, B, C, D	Audit and activity records of the observable occurrences (also referred to as an "event") significant and relevant to the security of DOJ information and information systems. These audit and activity records may include, but are not limited to, information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

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	X	Other	X
Other (specify): When components have completed the onboarding process, DOJ LaaS will collect user profile, contact information, and other PII necessary to create Splunk accounts.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Some of the audit logs DOJ LaaS ingests are received from other Federal government agencies that qualify to leverage DOJ's shared cybersecurity services, such as					

Government sources:
the Federal Retirement Thrift Investment Board (FRTIB), and the Court Services and Offender Supervision Agency (CSOSA). These agency customers may source information maintained on this system.

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): LaaS logs all access attempts to systems. By correlating user attempts to authorized users, a list can be generated of unauthorized users attempting to access systems. LaaS also collects web application logs from public facing DOJ websites.					

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	JMD OCIO CSS JSOC analysts, as well as members of the DOJ Insider Threat Program, have direct access to this system. Other entities within JMD receive access to such information on a case-by-case basis (for example, as part of incident response efforts).
DOJ Components	X		X	Information may be shared to other DOJ components on a case-by-case basis (for example, as part of incident response efforts). Splunk handles access to its data via role-based access. Integration with Splunk is via Active Directory Federated Services integrated Single Sign-On (SSO).

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		X	Information may be shared with other Federal entities on a case-by-case basis as authorized (for example, as part of incident response efforts, or as part of DOJ's shared cybersecurity services).
State, local, tribal gov't entities	X			Information may be shared with other state, local, and tribal government entities on a case-by-case as authorized (e.g., sharing incident response data).
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector	X		X	Information may be shared with the Department's private sector vendors, on a case-specific basis as authorized, for system administration, including but not limited to, tool service, and/or application troubleshooting.
Foreign governments				
Foreign entities				
Other (specify):	X			JMD may provide certain LaaS data to other entities, as required by law.

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.

DOJ LaaS information will not be released to the public for "Open Data" or for research or statistical analysis 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.

Individuals are notified that the account audit logs, and user records maintained in DOJ LaaS that manage system services are covered by are DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (7-14-2021).

Additionally, DOJ's website privacy policy informs visitors on DOJ public websites that, for site security purposes and to ensure that this service remains available to all users, the Department's information systems, and information systems operated by contractors on behalf of the Department, employ software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Anyone using these information systems expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, such evidence may be provided to appropriate law enforcement officials.

DOJ LaaS system users are required to sign an annual Rules of Behavior agreement, informing users that their IT, system, and network activities will be tracked. Such notice informs DOJ LaaS system users that tools like LaaS will track their IT, system, and network activities. Finally, upon accessing LaaS system, DOJ LaaS system users are presented with the following warning banner:

You are accessing a U.S. Government information system, which includes:

1. *this computer,*
2. *this computer network,*
3. *all computers connected to this network, and*
4. *all devices and storage media attached to this network or to a computer on this network.*

This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, and civil and criminal penalties. By using this information system, you understand and consent to the following:

- *You have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system. At any time, the government may monitor, intercept, search and/or seize data transiting or stored on this information system.*
- *Any communications transmitted through or data stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.*

For further information see the Department order on Use and Monitoring of Department Computers and Computer Systems.

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.

DOJ LaaS administrators will have access to the full range of administrative and system management information for the LaaS system. In such situation, DOJ LaaS administrators may have access to information collected from the tool and service applications. The purpose of access to this information is for system administration, maintenance, and continuity. Individuals will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to DOJ LaaS administrators.

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 are notified that the account, audit logs, and user records maintained in DOJ LaaS that manages system services can be accessed or amended, in accordance with DOJ regulations (28 C.F.R. Part 16, Subpart D), and in accordance with DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (7-14-2021).

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):** 10/17/2019, expiring 10/17/2022. If an ATO has not been completed, but is underway, provide status or expected completion date: **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**

	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The DOJ LaaS has vulnerability and configuration scans completed weekly. The Information System Security Officer (ISSO) performs continuous monitoring of the system through annual security control assessments and weekly audit log reviews. Suspicious account activities are reported to the System Owner.
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:** System authentication, privileged user activities, and account management event audit logs are collected in real-time and reviewed on a weekly basis by the ISSO.
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:** All DOJ users must complete computer security awareness training annually, as well as read and agree to comply with DOJ Information Technology Rules of Behavior both prior to accessing the DOJ network, and annually thereafter. System administrators, including DOJ LaaS administrators, must complete additional professional training, which includes security training.

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?

A full security control assessment has been completed for DOJ LaaS that includes physical, logical access, identification, authentication, vulnerability management, auditing, etc. The DOJ LaaS makes use of separate privileged and non-privileged user accounts, and leverages additional role-based access control technologies that allow for administrator session recording. All system and application log data are sent to DOJ's centralized audit log management system for triage and review. The DOJ LaaS system utilizes Transport Layer Security (TLS) encryption, which is a security protocol designed to facilitate privacy and data security for communications over the internet. This is compliant with the Federal Information Processing Standards

Publication (FIPS) 140-2,[6] to protect data in transit between the browser and user's workstation.[7] In addition, DOJ LaaS utilizes an Application Layer Firewall,[8] and integrated Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) technology[9] for inbound and outbound protection. The CSS ISSOs are charged with reviewing log-ins and performing auditing functions to ensure role-based access controls are satisfying the above measures.

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.)

Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule 3.2, for records created and maintained by Federal agencies related to protecting the security of information technology systems and data and responding to computer security incidents. Log data collected in Logging as a Service is captured in near real-time and is maintained for 365 days from the time of event generation.

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," 86 FR 37188 (7-14-2021).

Section 8: Privacy Risks and Mitigation

---

[6] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/projects/cryptographic-module-validation-program.
[7] User workstation is intended primarily to be used by one person at a time; they are commonly connected to a local area network and run multi-user operating system.
[8] Application Layer Firewall is a form of firewall that controls input, output, and/ or access from, to or by an application or service.
[9] The term Integrated IDS/IPS Technology refers to Intrusion detection system (IDS) which analyzes and monitors network traffic for signs that indicate attackers are using a known cyber threat. Intrusion Prevention System (IPS) proactively denies network traffic based on a security profile if that packet represents a known security threat.

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 DOJ LaaS captures and collects audit logs from DOJ federal information systems and as noted, federal agency information systems for agencies that use DOJ's shared cybersecurity services. Logs collected could include names, personal e-mail addresses, personal phone number, and device identifiers. The primary types of logs collected can be system/admin audit data. Possible logs that could be captured, include, but are not limited to, access information and credentials (e.g., passwords). All data retention is managed according to system owner requirements and associated policies. Data minimization strategies, including data retention, are determined on the tool, service, or application level. DOJ LaaS does not seek or request certain data sensitive types from its users (such as Social Security Numbers and Tax Identification Numbers) to minimize the collection of PII, although such data may be ingested.

There are certain privacy risks associated with the collection, use, access, dissemination, and maintenance of the PII that is collected. Some potential risks are identity theft, blackmail, physical harm, discrimination, and emotional distress.

Sources of information come directly from the users (government and contractors), systems automatically collecting information, from external government sources such as other Federal Government agencies, and logs from publicly facing DOJ sites. The DOJ LaaS implements encryption, account management, access controls, auditing, and system monitoring tools to mitigate privacy risks and protect PII, all in accordance with standards set by the National Institute for Standards and Technology (NIST). The DOJ LaaS makes use of Role-Based Access Control (RBAC),[10] while granting access for privileged and non-privileged user accounts. DOJ users (government and contractors), will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to DOJ LaaS administrators.

[10] RBAC is a method of restricting network access based on the roles of individual users within an enterprise. RBAC lets employees have access rights only to the information they need to do their jobs and prevents them from accessing information that does not pertain to them.

Information is shared on a case-by-case basis within the component, other DOJ components, other Federal agencies, and the private sector (for vendor-specific system troubleshooting) and via direct login by the DOJ LaaS administrators. In addition, other DOJ components do have direct login to Splunk search heads. This access is restricted based on user roles. The DOJ LaaS uses encryption and logging controls for risk mitigation purposes. The DOJ LaaS uses Transport Layer Security encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2, to protect data in transit between the browser and the user's workstation, uses an Application Layer Firewall and integrated IDS/IPS technology. The DOJ LaaS ISSO performs continuous monitoring of the security controls within the system to ensure security protections are operating as intended.

By Department Order, all DOJ users with access to Department networks, including DOJ LaaS, must complete an annual Cybersecurity Awareness Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the 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 established guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.

To ensure the continued relevance and effectiveness of security controls, risk assessments including privacy and security control assessments are routinely evaluated. In accordance with the NIST Special Publication 800-53, these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.