# United States Department of Justice
# Justice Management Division

# Privacy Impact Assessment
for the
Justice Enterprise Event Streaming System (JEESS)

Issued by:
Morton 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: February 18, 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 Department of Justice (DOJ) Enterprise Event Streaming System (JEESS) system is comprised of the enterprise Cribl Stream[1] application provided by Cribl, a security software and services company with headquarters in San Francisco, CA. Cribl Stream is a Commercial Off The Shelf (COTS) software that enables observability of data to allow the collection, enrichment, normalization, and routing of log data from multiple sources on DOJ networks to multiple DOJ log processing[2] and collection destinations. Observability is the practice that involves monitoring a systems output, e.g. logs and performance metrics, to understand the system's state. The Cribl Stream application is hosted on-premises within Pocatello, ID/Pocatello Information Technology Center (PITC)/Core Enterprise Facility-West (CEF-W) and Clarksburg, WV/Criminal Justice Information Services (CJIS) /Core Enterprise Facility-East (CEF-E) Datacenters.

DOJ aims to leverage JEESS to transform unstructured DOJ log and performance data into structured data before it is saved to persistent storage, e.g., magnetic or optical disks. The system can ingest multiple data formats into DOJ analytics tools from observability data sources and receive data from DOJ software-based log collection and endpoint monitoring agents and push-based[3] sources. It can schedule batch collection from multiple endpoints and Application Programming Interfaces (APIs) on DOJ networks. The system also supports existing processes for migration and normalization of logs and can recall the log data from low-cost storage. JEESS eliminates unnecessary data to control operational costs and improve system performance – such as duplicate fields, null (i.e., empty) values, and data elements that provide little analytical value. These services will allow the JEESS team to save on Security Information and Event Management (SIEM) licensing expenses. It will also allow the team to tag and segregate logs for DOJ enterprise Shared Services data sources (e.g., Office 365 logs, proxy data, etc.).

## 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 purpose of JEESS is to act as the DOJ's universal receiver and collect data from any observability data source (e.g., AWS, Azure, CrowdStrike, Splunk Enterprise, etc.) from all DOJ components;

---

[1] https://cribl.io/stream/
[2] 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.
[3] Pushed-based sources are hardware/software functions and services that send, or push, unsolicited data to a destination process or collection tool, e.g. Security Information and Event Management (SIEM), on a network.

eliminate unnecessary data; normalize[4] and enrich the data (adding metadata); route the data to DOJ analytical tools (e.g., Splunk Enterprise[5]). Cribl streams also allows the JEESS team to tag and segregate logs for the DOJ Shared Services team (e.g., O365 logs, proxy data, etc.). By not importing all required log files directly into Splunk Enterprise, DOJ will save log management licensing costs while simultaneously decreasing operational expenses. This streamlining of log management administration will free up Cybersecurity Services Staff (CSS) engineers for other operational and management tasks.

***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 | Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat 3073 |
| Executive Order | Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) |
| Federal regulation | |
| Agreement, memorandum of understanding, or other documented arrangement | Agreement must be executed between DOJ and Components subscribers which specifies the goods to be furnished or tasks to be accomplished by the Justice Management Division (JMD) Office of the Chief Information Officer (OCIO) Cybersecurity Services Staff (CSS) |
| Other (summarize and provide copy of relevant portion) | Office of Management and Budget (OMB) Circular No. A-130, OMB M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents, August 2021 |

## 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.***

[4] Normalization is a way to reorganize the data. This makes it easier for users to work with the data as it allows users to query and analyze the results.
[5] Splunk Enterprise is covered by the Logging as a Service PIA here: https://www.justice.gov/d9/2024-08/pia-jmd-doj_logging_as_a_service_laas_final.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 |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A and B | Names are required for a Cribl account creation as the system is integrated with DOJLogin. |
| **Date of birth or age** | | | |
| **Place of birth** | | | |
| **Gender** | | | |
| **Race, ethnicity, or citizenship** | | | |
| **Religion** | | | |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | A, B, C, D | It is not the intent of Cribl Stream to collect Social Security Numbers, however, logs may contain SSN. JEESS system does not store any data while routing logs to Splunk. |
| **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 | JEESS is used to collect, normalize, and route mail server logs to the DOJ JMD Splunk Enterprise system where they are ingested and retained for analysis. The logs may contain business contact information, email addresses, phone numbers, and/or an address of a business. |
| **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** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| **Legal documents** | | | |
| **Device identifiers, e.g., mobile devices** | X | A | JEESS is used to collect, normalize, and route mail server logs to the DOJ JMD Splunk Enterprise system where they are ingested and retained for analysis. These logs pertain to AirWatch logs (logs from mobile devices) may contain user identifying information such as name, organization, and phone number. |
| **Web uniform resource locator(s)** | | | |
| **Foreign activities** | X | A,B,C,D | Depending on the security tool/application, JEESS 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** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public - Non-USPERs | (4) Comments |
|---|---|---|---|
| - **Voice recording/signatures** | | | |
| - **Scars, marks, tattoos** | | | |
| - **Vascular scan, e.g., palm or finger vein biometric data** | | | |
| - **DNA profiles** | | | |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | X | A, B | JEESS collects relevant security logs to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and /or data of access. It is not the intent of the system to log passwords however it may occur while ingesting logs for other systems.<br><br>Incident Response Plan (IRP) logs will be collected with JEESS and will be sent to Splunk Enterprise for retention and analysis. |
| - **User ID** | X | A and B | JEESS collects IRP related logs. |
| - **User passwords/codes** | X | A and B | JEESS transmits passwords for user accounts when federated authentication is not available. Otherwise, user password is logged by a system outside of JEESS. The system may log those passwords, although that is not the intent. |
| - **IP address** | X | A, B, C and D | JEESS collects IRP related logs. |
| - **Date/time of access** | X | A, B, C and D | JEESS collects IRP related logs. |
| - **Queries run** | | | |
| - **Contents of files** | | | |
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C and 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): For new JEESS users, DOJ JEESS will collect 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). This is the same audit logs collected by LaaS (Splunk), please see reference below. [6] | | | | | |

| **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 for DOJ JEESS are received from other Federal government agencies that qualify to leverage DOJ's shared cybersecurity services such as Microsoft 365. | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | x | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): JEESS collects similar information as LaaS. JEESS collects audit logs from systems, computing appliances, and applications. | | | | | |

## 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.***

[6] Privacy Impact Assessment for DOJ Login as a Service (Splunk)

| 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 | | | Data that traverse through JEESS will be sent to Logging as a Service (LaaS) where JMD OCIO CSS Justice Security Operations Center (JSOC) analyst(s) as well as member(s) of the DOJ Insider Threat Program have direct access to the data. Other entities within JMD receive access to such data on a case-by-case basis (e.g., as part of an Incident response effort). |
| DOJ Components | X | | | Data maybe shared with other DOJ components on a case-by-case basis (e.g., as part of an incident response effort).<br>Data can also be shared with DOJ components that have their own SIEM environment on request basis. |
| Federal entities | X | | | Data may be shared with other Federal entities on a case-by-case basis as authorized (e.g., as part of an incident response effort) or as part of DOJ shared cybersecurity services. |
| State, local, tribal gov't entities | X | | | Data 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 | | | | |

| 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 | | | Data may be shared with the Department private sector vendor, on a case-by-case 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 data that traverse though JEESS 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.***

JEESS 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.***

JEESS ingests audit log information and sends the audit log information to DOJ Logging as a Service (LaaS). JEESS leverages the notification provided to individuals 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 Fed. Reg. 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.

JEESS leverages the DOJ LaaS annual requirement, 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 JEESS system, DOJ JEESS system users are presented with the following warning banner:

You are accessing U.S. Government information technology and/or information systems which includes: (1) this information technology, (2) this information system, (3) all information technology devices connected to this network, and (4) all devices and storage media attached to this information system or to information technology on this network.

This information technology and information system is provided for U.S. Government authorized use only. You have no reasonable expectation of privacy when using this information technology and/or information system and the government may monitor, intercept, search and/or seize data transiting through or stored within. Unauthorized or improper use may result in disciplinary action as well as civil and/or criminal penalties.

***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.***

None. Individual are required to adhere to the collection, use or dissemination of information in the system per Rules of Behavior that they sign to gain access to the system.

***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.***

JEESS Cribl does not maintain any data nor is it the originating source of the individual's data. However, if an individual wanted to gain access to their data will have to contact the DOJ LaaS program. 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 Fed. Reg. 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):**<br>12/04/2024 – 12/04/2025<br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br>**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 | **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: Moderate** |
| x | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**<br>The JEESS 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 by the ISSO. |
| 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:**<br>Prior to accessing the DOJ network and annually thereafter, all DOJ users must complete computer security awareness training and comply with DOJ Information Technology Rules of Behavior. JEESS system administrators must complete additional professional training, which includes more in-depth security training for privileged users on the 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?***

A full security control assessment has been completed for JEESS that includes physical, logical access, identification, authentication, vulnerability management, auditing, etc. JEESS makes use of privileged accounts and leverages additional role-based access control technologies that allow for administrator session recording. The DOJ JEESS system utilizes Transport Layer Security (TLS) encryption, which is a security protocol designed to facilitate privacy and data security for communications over the internet. TLS encryption is used to protect data in transit for the user's browser session while accessing the JEESS Application. In addition, JEESS utilizes an Application Layer Firewall, and integrated Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) technology for inbound and outbound protection. The CSS ISSOs are charged with reviewing logins 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 JEESS system are not retained. JEESS ingests the audit logs and send those logs to DOJ LaaS which 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.

## 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:***

DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 Fed. Reg. 37188 (7-14-2021), and JMD-026, "Security Monitoring and Analytics Service Records", 86 FR 41089 (7-30-2021).

## 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.***

JEESS 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. JEESS 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, and from external government sources such as other Federal Government agencies. The DOJ JEESS 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 JEESS makes use of Role-Based Access Control (RBAC), 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 JEESS administrators.

By Department Order, all DOJ users with access to Department networks, including DOJ JEESS, 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 employee or contractor access revocation to DOJ computing resources (e.g. computers, applications, and networks). Continued violations can lead to termination of employment for the DOJ employee or contractor. 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.