United States Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Cloud Logging as a Service (Cloud LaaS)

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

Approved by: Peter A. Winn
Chief Privacy and Civil Liberties Officer (A)
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: 11/18/2023

(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 or Department) Cybersecurity Services Staff (CSS) enters into agreements to provide information technology services to external federal government agency customers. As part of these agreements, Cloud Logging as a Service (Cloud LaaS or C-LaaS) provides audit log and monitoring services to certain External Federal Agency (EFA) subscribers. Cloud LaaS receives and ingests logs from these EFAs. The Cloud LaaS application 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[1] and monitoring for the EFAs. Cloud LaaS aims to make machine data accessible across an organization and identifies data patterns, provides metrics, diagnoses problems, and provides decision support for business operations. Cloud LaaS can analyze data from on-premises, virtualized environments, or cloud-based deployments.

Cloud LaaS provides the Splunk Enterprise Software in a cloud environment using a purely Software as a Service (SaaS) based infrastructure and monitoring functionality where setup and management of the support infrastructure is performed by Splunk Cloud Operations. Cloud LaaS is a software platform to search, analyze, and visualize the machine-generated data gathered from the websites, applications, sensors, devices, and other components that comprise the IT infrastructure of the agencies using these services.

Because Cloud LaaS capture and analyze substantial amounts of personally identifiable information (PII), a privacy impact assessment is required by Section 208 of the E-Government Act of 2002.

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 C-LaaS is to index collected data from disparate security devices and "normalize" the data—that is, make it easier to review and analyze. Collection of this data provides DOJ's Justice Security Operations Center (JSOC) analysts a "single pane of glass" to monitor EFAs networks. The C-LaaS systems ingest and indexes data from EFAs throughout the organization. EFAs-owned Splunk Heavy Forwarders and Universal Forwarders sit in the external subscriber environment. These

[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.

forwarders send EFA application/infrastructure logs to the C-LaaS servers (Splunk Heavy Forwarders or Indexers). The C-LaaS Splunk Indexers receive, index, and store incoming data from the forwarders per preset configurations. Configurations are controlled and updated through the C-LaaS Deployment Server which is restricted to the C-LaaS Team.

The C-LaaS 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 C-LaaS 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 provide the ability to query data and create dashboards, alerts, and reports. All events are monitored by JSOC analysts.

Splunk users gain access to data on the Indexers through the Splunk Search Heads based on the user's approved level of access. To gain access to a Splunk Search Head, users must complete Splunk Fundamentals 1 training. The training ensures that they know how to correctly create and execute searches. As a note, the JSOC and the DOJ Insider Threat Program have access to all logs per Department policy to meet security requirements. C-LaaS administrators and CSS engineers (including federal employees and contractors) are the only individuals who have access to the back-end database.

Only the JSOC and the DOJ Insider Threat Program have access to all the DOJ Component data. Access to this data allows for the support of network monitoring, incident response and investigation roles. That data is used to correlate network, application, and user activity across the EFAs.

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;

	40 U.S.C. 1441
Executive Order	Executive Order 14028
Federal regulation	OMB M-21-31
Agreement, memorandum of understanding, or other documented arrangement	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)	Office of Management and Budget (OMB) Circular No. A-130; DOJ Order 0904: Cybersecurity Program

<u>Section 3</u>: 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). <u>Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.</u>

(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, D	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)	X	A, B, C, D	It is not the intent of Splunk to collect SSNs. SSNs may be inadvertently collected if they are traversing the network but, if identified, the source will be found and the issue fixed.
Tax Identification Number (TIN)			
Driver's license			

(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

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, emails to or from the agency may include this personal information.
Personal phone number	X	A, B,C,D	Mail server logs are ingested into Splunk; therefore, anyone sending emails to or from the agency may include this personal information
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			
Device identifiers, e.g., mobile devices	X	A, B	Mobile device logs may contain user identifying information such as a 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			

(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

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**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A, B	Splunk collects Incident Response (IR) related logs to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and/or date of access.
- **User ID**	X	A, B	Splunk collects Incident Response (IR) related logs to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and/or date of access.
- **User passwords/codes**			

(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

- **IP address**	X	A, B	Splunk collects Incident Response (IR) related logs to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and/or date of access.
- **Date/time of access**	X	A, B	Splunk collects Incident Response (IR) related logs to support compliance and the JSOC. This includes a combination of user IDs, IP addresses, and/or date of access.
- **Queries run**	X	A, 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.
- **Contents of files**			
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 the external agency 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. In addition, as mail server logs are ingested into Splunk, emails to or from the agency may include other personal information.

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 (specify): Upon external customers completing the onboarding process, C-LaaS will collect user profile, contact information, and other PII necessary to create Splunk accounts.					

Government sources:					
Within the Component		Other DOJ Components		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): C-LaaS provides audit log services to ingest and receive logs from External Federal Government Agencies. These Federal Government agency customers' information is maintained on the system.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): C-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. C-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				
DOJ Components				

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	It is the intent of C-LaaS to provide audit log services to EFAs enrolled in the CSS service offering. System Administration/ Monitoring Services will provide logs/access, in accordance with Section 6 below. Information will be shared with the EFAs.
State, local, tribal gov't entities	X			Case-by-case for incident response data sharing purposes
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector	X			Information may be shared with the Department's private sectors services vendors, on a case-specific basis, for system administration, including, but not limited to, tool service, and/or application troubleshooting.
Foreign governments				
Foreign entities				
Other (specify):	X			As required by law. This service is managed by DOJ JSOC and offered to agencies external to DOJ. Data will be shared with JSOC admins for monitoring purposes and the enrolled agency POCs.

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.

C-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.

Notice is not required because the PII in these systems do not constitute "records in systems of records" under the Privacy Act of 1974. That said, DOJ recommends to its customers warning banner language that can be used. The EFAs can also leverage their own agency's standardized warning banner using the recommended language.

The account audit logs and user records maintained in C-LaaS that manage system services are covered by JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (July 14, 2021), and JUSTICE/JMD-026, *Security Monitoring and Analytics Service Records*, 86 FR 41089 (July 30, 2021).

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.

C-LaaS Administrators will have access to the full range of administrative and system management information for the LaaS system. In such situations, C-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 C-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.

Access is not required because the PII in these systems do not constitute "records in systems of records" under the Privacy Act of 1974.

The purpose of access to this information is for system administration, maintenance, and continuity. No procedures exist for individuals to be provided an opportunity to gain access to, or to request amendment or correction of, information in C-LaaS.

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):** **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:** ATO date: 10/13/2022, expiring 10/13/25.
	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:** Based on the FIPS 199 information types identified for the C-LaaS information system the information system has a security categorization of Moderate.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The C-LaaS has vulnerability and configuration scans completed monthly by the Cloud Service Provider (Splunk.) 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:** Audit logs are collected daily. Logs are reviewed by the external subscriber in accordance with their Agency/Department security and privacy standards.
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 and EFA users must complete computer security awareness training annually, as well as read and agree to comply with information system information technology Rules of Behavior both prior to accessing the DOJ network, and annually thereafter. System

	administrators, including C-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 C-LaaS to include physical, logical access, identification, authentication, vulnerability management, auditing, etc. The C-LaaS makes use of separate Privileged, Non-Privileged user accounts and uses additional role-based access control technologies that allow for administrator session recording. All system and application log data (enrolled in the service) are being sent to the centralized audit log management system for triage and review. The C-LaaS system utilizes Transport Layer Security encryption. This is compliant with the Federal Information Processing Standards Publication (FIPS) 140-2[2], to protect data in transit between the browser and user's workstation. C-LaaS has also implemented FIPS validated encryption for data stored at rest. In addition, C-LaaS utilizes the use of Application Layer Firewall[3], integrated Intrusion Detection System (IDS)/ Intrusion Prevention System (IPS)[4] technology for any inbound and outbound protection.

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 incident. Log data is maintained in Logging as a Service as the DOJ's repository for 365 days. See 64 FR 73585 (Dec. 30, 1999).

<u>Section 7</u>: 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

[2] FIPS 140-2 can be found here: https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

[3] Application Layer Firewall is a form of firewall that controls input, output, and/ or access from, to or by an application or service.

[4] 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.

in a "system of records," as defined in the Privacy Act of 1974, as amended).

__X___ No. __-_ Yes.

7.2 ***Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:***

To the extent that any records in the system constitute records in a system of records under the Privacy Act, the appliable SORNs are: JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (July 14, 2021), and JUSTICE/JMD-026, *Security Monitoring and Analytics Service Records*, 86 FR 41089 (July 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.***

The C-LaaS captures and collects audit logs from External Federal Agencies' (EFA) information systems. Logs collected could include names, personal e-mail addresses, personal phone number, and device identifiers. The primary types of logs collected are system/admin audit data. Possible logs that could be captured are 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. The C-LaaS does not collect certain data types for its users (such as Social Security Numbers and Tax Identification Numbers) to minimize the collection of PII.

Sources come directly from the users (government and contractors), systems automatically collecting information, and from external government sources such as other Federal Government agencies. The C-LaaS implements encryption, account management, access controls, auditing, and system monitoring tools to mitigate risk and protect privacy information. The C-LaaS makes use of role-based access control (RBAC)[5], pertaining to access granted for privileged and non-privileged user accounts. EFAs will not be provided an opportunity to voluntarily participate in the collection, use, or dissemination of information accessible to C-LaaS Administrators.

Information is shared on a case-by-case basis to private sector (for vendor-specific system troubleshooting) and via direct login by the C-LaaS administrators. In addition, other EFAs have direct login to Splunk search heads. This access is restricted to only those with proper role(s). The C-LaaS uses encryption and logging controls for mitigation purposes. The C-LaaS make use of 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 and makes use of Application Layer Firewall and integrated IDS/IPS technology. The C-LaaS ISSO performs continuous monitoring of the security controls within the system to ensure security protection are operation as intended.

All EFA users (and DOJ System Administrators) with access to the information systems network, including C-LaaS, must receive an annual Cybersecurity Awareness Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course identifies potential risks and vulnerabilities associated with using the IT systems, provides a review of the user's role in protection 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 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 EFA computers. Participation in the training course is tracked by the EFA.

To ensure the continued relevance, effectiveness of security controls, risk assessments including privacy and security control assessments are routinely evaluated. In accordance with the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 (Rev.5), these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.

[5] 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.