United States Department of Justice
Justice Management Division

# Privacy Impact Assessment
for the
Cyber Operations System

Issued by:
Morton Posner
JMD Senior Component Official for Privacy

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

Date approved: August 9, 2023

*(May 2019 DOJ PIA Template)*

## Section 1: Executive Summary

The United States Department of Justice (DOJ or "the Department"), Justice Management Division (JMD), Office of the Chief Information Officer (OCIO), Cybersecurity Services Staff (CSS), Cyber Operations (CyberOps) information system consists of five commercially available off-the-shelf (COTS) software products that allow DOJ to automate the detection, intake, tracking, and updating of security incident information. The five COTS software products are as follows:

- Jira: A collaboration software program used to ingest, track, and share security incident data and provide incident ticketing. Jira ingests data from the Splunk system[1] and can create security incident cases via a process called "triage," whereby Splunk performs searches for indicators of malicious computer activity, creates alerts, sends alerts to Jira, and Justice Security Operations Center (JSOC) analysts review them.
- Confluence: A collaboration software program used to create, organize, and share documents.
- Anomali Threat Stream: A source for cyber threat intelligence that provides correlation match capabilities against the Department's security telemetry data (data collected from a network environment that can be analyzed to monitor the health and performance, availability, and security of the network and its components) for review by the Department's intelligence analysts.
- Anomali Integrator: A local integration with the Enterprise Logging as a Service/Security Information and Event Management system[2] that ingests indicators of compromise identified by the Department's intelligence analysts.
- GitHub: A software development platform that provides version control for programmers writing software.

DOJ has modified these five COTS software products for DOJ use, which are hosted within the DOJ Secure Enclave.[3] CyberOps is used by an entity within JMD OCIO CSS, the JSOC, to automate security incident processes, including the intake, tracking, and updating of security incident information for DOJ Components and other government customers of its Shared Services. Shared Services customers are federal agencies outside of the Department that leverage the DOJ's cybersecurity services through an interagency agreement with the Department. CyberOps will also provide JSOC with cyber threat information and software development tools.

JMD has prepared a Privacy Impact Assessment (PIA) for CyberOps because this system will collect and maintain Personally Identifiable Information (PII). Specifically, CyberOps will collect and maintain information related to security incidents that impact DOJ information technologies (IT), information systems (IS), and networks, including but not limited to: identifiers and contacts for any person reporting, responding to, or associated with a reported incident; unique identifiers assigned to a

---

[1] DOJ uses Splunk to collect, store, query, and correlate machine logs. Splunk uses this information to generate graphs, reports, and alerts in support of the Department's audit logging and monitoring in support of security operations. Splunk is covered by the Logging as a Service PIA here: https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.

[2] The Enterprise Logging as a Service/Security Information and Event Management system is covered under separate privacy documentation available at: https://www.justice.gov/opcl/doj-privacy-impact-assessments.

[3] Secure Enclave is covered by a separate privacy impact assessment available at: https://www.justice.gov/opcl/doj-privacy-impact-assessments.

DOJ IT, IS, network user, or any person attempting to access (whether authorized or unauthorized) these systems and technologies, including Internet Protocol (IP) addresses, unique device addresses, usernames, hostnames, e-mail addresses, or other related information.

## 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 JMD OCIO CSS supports and secures the DOJ and its components by providing cybersecurity leadership across the Department. CyberOps allows JSOC to triage and respond to incidents across the Department and Shared Services customers with integrated threat information. To support the DOJ mission, thousands of events need to be reviewed each day and hundreds of security incidents need to be tracked and closed in order to maintain a strong security posture.

CyberOps information system is the security ticketing system for the DOJ and any Shared Services customers. CyberOps is used to track investigations into all potential security incidents within DOJ's and the Shared Services customer's purview including breaches.[4] Components, Shared Services customers and the JSOC use this system to collaborate on and share documentation pertaining to these security incidents and bring them to a resolution. The bulk of potential PII information is collected in the course of these investigations. Each ticket is saved as a record of the investigation and its resolution, for later reference.

***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;<br><br>40 U.S.C. 1441 note, requiring Federal Agencies to plan for the security and privacy of their computer systems |
| | Executive Order | Executive Order 14028 of May 12, 2021, Improving the Nation's Cybersecurity |
| | Federal Regulation | |

[4] A breach is a type of security incident that results in "the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses [PII] or (2) an authorized user accesses or potentially accesses [PII] for another than authorized purpose." OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (Jan. 3, 2017).

| | | |
|---|---|---|
| | Agreement, memorandum of understanding, or other documented arrangement | |
| | | U.S. Department of Justice 0601 – DOJ Order Privacy and Civil Liberties<br><br>U.S. Department of Justice DOJ Order 0904 - CYBERSECURITY PROGRAM<br><br>DHS Privacy Policy Guidance Memorandum 2017-01, DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information (April 2017)<br><br>OMB Circular A-130 - Managing Information as a Strategic Resource (July 28, 2016)<br><br>OMB Memorandum M-17-12 - Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017)<br><br>OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003)<br><br>OMB Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006)<br><br>OMB Memorandum M-11-02, Sharing Data While Protecting Privacy (November 3, 2010)<br><br>OMB Memorandum M-13-13, Open Data Policy<br><br>OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government |
| | Other (summarize and provide copy of relevant portion) | OMB Memorandum 17-09, Management of Federal High Value Assets |

## 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:<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 |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | A, B, C, and D | Contact roster of JSOC personnel.<br><br>Additionally, while CyberOps does not routinely collect this type of PII; PII may be included in reported actual or suspected security incidents being investigated if necessary and relevant to the incident. |
| **Date of birth or age** | X | A, B, C, and D | While CyberOps does not routinely collect this type of PII; PII may be included in reported actual or suspected security incidents being investigated if necessary and relevant to the incident. |
| **Place of birth** | X | A, B, C, and D | See comment above. |
| **Gender** | X | A, B, C, and D | See comment above. |
| **Race, ethnicity or citizenship** | X | A, B, C, and D | See comment above. |
| **Religion** | X | A, B, C, and D | See comment above. |
| **Social Security Number (full, last 4 digits or otherwise truncated)** | X | A, B, C, and D | See comment above. |
| **Tax Identification Number (TIN)** | X | A, B, C, and D | See comment above. |
| **Driver's license** | X | A, B, C, and D | See comment above. |
| **Alien registration number** | X | A, B, C, and D | See comment above. |
| **Passport number** | X | A, B, C, and D | See comment above. |
| **Mother's maiden name** | X | A, B, C, and D | See comment above. |
| **Vehicle identifiers** | X | A, B, C, and D | See comment above. |

| (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 |
|---|---|---|---|
| **Personal mailing address** | X | A, B, C, and D | Contact roster of JSOC personnel, which may include personal contact information.<br><br>Additionally, while CyberOps does not routinely collect this type of PII; PII may be included in reported actual or suspected security incidents being investigated if necessary and relevant to the incident. |
| **Personal e-mail address** | X | A, B, C, and D | See comment above. |
| **Personal phone number** | X | A, B, C, and D | See comment above. |
| **Medical records number** | X | A, B, C, and D | While CyberOps does not routinely collect this type of PII; PII may be included in reported actual or suspected security incidents being investigated if necessary and relevant to the incident. |
| **Medical notes or other medical or health information** | X | A, B, C, and D | See comment above. |
| **Financial account information** | X | A, B, C, and D | See comment above. |
| **Applicant information** | X | A, B, C, and D | See comment above. |
| **Education records** | X | A, B, C, and D | See comment above. |
| **Military status or other information** | X | A, B, C, and D | See comment above. |
| **Employment status, history, or similar information** | X | A, B, C, and D | See comment above. |
| **Employment performance ratings or other performance information, e.g., performance improvement plan** | X | A, B, C, and D | See comment above. |
| **Certificates** | X | A, B, C, and D | See comment above. |
| **Legal documents** | X | A, B, C, and D | See comment above. |
| **Device identifiers, e.g., mobile devices** | X | A, B, C, and D | See comment above. |
| **Web uniform resource locator(s)** | X | A, B, C, and D | See comment above. |
| **Foreign activities** | X | A, B, C, and D | See comment above. |
| **Criminal records information, e.g., criminal history, arrests, criminal charges** | X | A, B, C, and D | See comment above. |
| **Juvenile criminal records information** | X | A, B, C, and D | See comment above. |

| (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 |
|---|---|---|---|
| **Civil law enforcement information, e.g., allegations of civil law violations** | X | A, B, C, and D | See comment above. |
| **Whistleblower, e.g., tip, complaint or referral** | X | A, B, C, and D | See comment above. |
| **Grand jury information** | X | A, B, C, and D | See comment above. |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | X | A, B, C, and D | See comment above. |
| **Procurement/contracting records** | X | A, B, C, and D | See comment above. |
| **Proprietary or business information** | X | A, B, C, and D | See comment above. |
| **Location information, including continuous or intermittent location tracking capabilities** | X | A, B, C, and D | See comment above. |
| ***Biometric data:*** | | | |
| - **Photographs or photographic identifiers** | X | A, B, C, and D | See comment above. |
| - **Video containing biometric data** | X | A, B, C, and D | See comment above. |
| - **Fingerprints** | X | A, B, C, and D | See comment above. |
| - **Palm prints** | X | A, B, C, and D | See comment above. |
| - **Iris image** | X | A, B, C, and D | See comment above. |
| - **Dental profile** | X | A, B, C, and D | See comment above. |
| - **Voice recording/signatures** | X | A, B, C, and D | See comment above. |
| - **Scars, marks, tattoos** | X | A, B, C, and D | See comment above. |
| - **Vascular scan, e.g., palm or finger vein biometric data** | X | A, B, C, and D | See comment above. |
| - **DNA profiles** | X | A, B, C, and D | See comment above. |
| - **Other (specify)** | | | |
| ***System admin/audit data:*** | | | |
| - **User ID** | X | A, B, C, and D | Routine audit information on user and system activity.<br><br>System admin/audit data in reported actual or suspected security incidents being investigated if necessary and relevant to the incident. |
| - **User passwords/codes** | X | A, B, C, and D | See comment above. |
| - **IP address** | X | A, B, C, and D | See comment above. |
| - **Date/time of access** | X | A, B, C, and D | See comment above. |
| - **Queries run** | X | A, B, C, and D | See comment above. |
| - **Content of files accessed/reviewed** | X | A, B, C, and D | See comment above. |
| - **Contents of files** | X | A, B, C, and D | See comment above. |

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to:<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 |
|---|---|---|---|
| **Other (please list the type of info and describe as completely as possible):** | X | A, B, C, D | Designated and cleared users from the JSOC, Security staff of other components, and Secure Enclave administrators, will be able to access information stored and processed in the application. Secure Enclave administrators will have access to the full range of administrative and system management information for CyberOps.<br><br>Security incidents captured by CyberOps may include personal information relating to the substantive work of DOJ. Because of the varied nature of the Department's work and because email messages and documents captured could conceivably include almost any type of PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. |

### *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 | X | Email | X | Other | X |
| Other (specify): Individuals will directly provide, or security systems will automatically collect, user profile information, contact information, and other PII necessary and relevant to identification of, and investigations into, security incidents within the DOJ network. | | | | | |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| Within the Component | X | Other DOJ Components | X | Online | |
| State, local, tribal | | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | | | |
| Other (specify): JMD offers access to the CyberOps ticketing system to other federal agencies as part of its Shared Services offering. These customers are able to submit, read and manage incident tickets related only to their own organization. | | | | | |

| **Non-government sources:** | | | | | |
|---|---|---|---|---|---|
| Members of the public | X | Public media, Internet | | Private sector | |
| Commercial data brokers | | | | | |
| Other (specify): While rare, in the event that an outside organization sent PII relating to members of the public to a DOJ component and this resulted in a PII breach, this information could be ingested into the ticketing system and retained as a record. Additionally, some components process PII for members of the public in their daily duties (for example, concealed carry permit requests and the requisite background information for such a request). These could also potentially be part of an incident if not handled appropriately by the component or successfully targeted by a cyber-attack. | | | | | |

## 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 | System administration and audit log information as needed to ensure operability of CyberOps, in accordance with Section 6, below. Information may be shared within JMD on a case-by-case basis as |

| 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.** |
| | | | | part of incident response efforts. |
| DOJ Components | X | | X | Information may be shared with other DOJ components on a case-by-case basis as part of incident response efforts, e.g., the Office of Privacy and Civil Liberties (OPCL). Designated IT Security POC's at each component also have access to the ticketing system portion of CyberOps and can view security incident tickets that relate to their component. |
| Federal entities | X | | X | Information may be shared with other Federal entities on a case-by-case basis as part of incident response efforts. Designated IT Security POC's at each Shared Services customer also have access to the ticketing system portion of CyberOps and can view security incident tickets that are assigned to their component. |
| State, local, tribal gov't entities | X | | | Information may be shared with a State, local, or tribal government entity on a case-by-case basis as part of incident response efforts. |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | X | | | A court or other judicial tribunal may request incident document for litigation purposes. |
| Private sector | X | | | Vendors providing support on the system, to the extent necessary to provide such support. |
| Foreign governments | | | | |
| Foreign entities | | | | |
| Other (specify): | X | | | 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.***

CyberOps information will not be released to the public for "Open Data" or for research or statistical analysis or any other 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 have been notified that the account, audit log, and user records maintained in Secure Enclave, to include Cyber Operations, are covered by JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records,[5] last published in full at 86 Fed. Reg. 37188 (July 14, 2021).

Additionally, each user must sign a Rules of Behavior (ROB) prior to gaining access to DOJ systems. The ROB defines what constitutes improper use and describes, in detail, the proper handling and storage of PII within the network and beyond. Furthermore, each time a user attempts to access any DOJ information system (laptop, desktop) they receive a banner that states the system is part of the DOJ network, that the user has no reasonable expectation to privacy on the system, and that improper use of the system or connected network will result in disciplinary action. A similar banner is shown again when connecting to the VPN to access the system remotely. Cyber Operations is not accessible outside of the DOJ Enterprise Network and is not accessible to the public.

***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.***

Individuals using the CyberOps system must consent to collection of data as described in the Rules of Behavior and the applicable User Agreement before accessing DOJ IT, information systems, or networks. Since CyberOps is hosted on the Secure Enclave, Secure Enclave Administrators will have access to the full range of administrative and system management

[5] With regards to Section 5, other notices and procedures to allow individuals access to information in the system pertaining to them may apply, depending on the nature of information maintained in the tools, services, and applications, and how the information is retrieved. The tools, services, and applications hosted by the Secure Enclave will have their own privacy compliance document, as required.

information for the servers hosting the CyberOps system. In such a situation, Secure Enclave administrators may have access to information from the CyberOps system for the purpose of 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 Secure Enclave and CyberOps Administrators.

CyberOps is used to collect information and evidence about incidents that may impact other DOJ systems. The Rules of Behavior and the applicable User Agreements for those other DOJ systems require consent to the collection or specific uses of their user's information.

***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 have been notified that the account, audit log, and user records maintained in Secure Enclave, to include Cyber Operations, that are used to plan and manage system services can be accessed or amended in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (July 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>07/12/2021 (3 years)<br>If an ATO has not been completed, but is underway, provide status or expected completion date: |
| | 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:<br>CyberOps has vulnerability and configuration scans completed monthly and weekly. |
| 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: |

| | |
|---|---|
| | JSOC-Security Tools audit logs are aggregated and viewed through ArcSight which is continually monitored by an ArcSight analyst. |
| 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>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 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?***

CyberOps has a security categorization of FISMA Moderate, and DOJ has implemented all applicable privacy and security controls for a Moderate baseline. A full security control assessment has been completed for CyberOps, to include physical and logical access, identification and authentication, vulnerability management, and auditing. CyberOps supports the use of PIV authentication to the incident ticketing and evidence collection repository that could store PII. Access to the repository is limited to JSOC analysts and SOC analysts from the DOJ components and Shared Services customers. Analyst permissions within the repository are determined by role-based access controls that are managed by JSOC engineers. Component and customer users can only access incident tickets assigned to their component while JSOC analysts have access to all tickets at the JSOC/oversight level and the individual components. All users of the repository are required to manually zip and encrypt any PII collected as evidence before it is entered into the system.

Because CyberOps will be maintained within the DOJ Secure Enclave, CyberOps will also utilize the technical safeguards implemented within Secure Enclave. For example, CyberOps leverages additional role-based access control technologies. All system and application log data is sent to DOJ's centralized audit log management system for triage and review. CyberOps applications make use of Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2,[6] to protect data in

[6] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/groups/STM/cmvp/standards.html.

transit between the browser and the user's workstation. The user's workstation[7] makes use of Application Layer Firewall[8] and integrated IDS/IPS[9] technology and encapsulates in an Internet Protocol Security Virtual Private Network[10] (IPSEC VPN) all data replication/transit between the two Secure Enclave datacenters. The CSS Information Security System Officers (ISSOs) are charged with reviewing logins and performing auditing functions to ensure role-based access controls 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 is maintained in Logging as a Service as the DOJ's repository for 365 days (unless retained longer for investigative or similar purposes).

## Section 7: Privacy Act

***7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).***

____ No. __X__ Yes.

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

JUSTICE/DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, last published in full at 86 Fed. Reg. 37188 (July 14, 2021).

---

[7] A 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 systems.
[8] An "Application Layer" firewall is a form of firewall that controls input, output, and/or access from, to or by an application or service.
[9] An Intrusion Detection System (IDS) 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.
[10] Internet Protocol Security, or "IPSEC," is "a framework of open standards for ensuring private communications over public networks and is "typically used to create a virtual private network." NIST SP 800-77, *Guide to IPsec VPNs* (Dec. 2005). A Virtual Private Network, or "VPN," is a "virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks." *Id.*

## 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 the***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

CyberOps contains the primary ticketing and evidence collection repository for all DOJ Security Incidents, to include PII breaches and potential breaches. PII would be collected in the course of an investigation and retained as evidence. Most commonly this is contact information relating to the individual reporting the issue but can include other information as the incident is investigated. This can include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (user IDs, user passwords, IP addresses, date/time of actions, queries run, contents of files), and other data such as hostname, email contents, and connection attempts as it pertains to potential security incidents. Because of the varied nature of the Department's work and because email messages and documents captured could conceivably include almost any type of PII, it is not possible to list with certainty every item of information that will be collected, maintained, or disseminated by the system. As a result, CyberOps risks collection and maintaining more PII than is relevant and necessary to address the security incident. The Department has put in place administrative and technical measures to mitigate privacy risks. All data for security incidents is retained as an official record of the investigation. CyberOps and the JSOC does not routinely collect certain data types for its users (such as Social Security numbers and Tax Identification Numbers) to minimize the collection of PII.

Because of the investigatory nature of security incidents, it is not possible for JMD in all instances to assess the relevancy and/or necessity of PII in the early stages of incident reviews. To mitigate such risks, JMD generally sources information within CyberOps directly from users (government and contractors), systems automatically collecting information, and from external government sources such as other Federal Government agencies where the JSOC and the ticketing system is offered as a service. Information is only shared on a case-by-case basis within the component, with other DOJ Components, other Federal agencies, and in rare instances, the private sector (for vendor-specific system troubleshooting), and via direct login by the Secure Enclave administrators.

Given the sensitive nature of DOJ incident monitoring and investigations, DOJ must safeguard CyberOps against unauthorized uses. To mitigate such risks, the Secure Enclave implements

encryption, account management and access controls, auditing, and system monitoring tools to mitigate and protect PII as the hosting service. The Secure Enclave makes use of separate Privileged and Non-Privileged user accounts and access is granted on least privilege and need-to-know requirements. DOJ users (government and contractors) will not be provided an opportunity to voluntarily participate in the collection, use or dissemination of information accessible to Secure Enclave Administrators (although they agree to a Rules of Behavior and regularly receive notices of IT access to and uses of PII). Designated IT security personnel have access to the security incident tickets and information therein that pertain to their component via the ticketing system in CyberOps. The Secure Enclave hosts CyberOps and uses encryption and logging controls for mitigation purposes. The Secure Enclave makes use of SSL encryption, compliant with the FIPS 140-2, to protect data in transit between the browser and the user's workstation, makes use of Application Layer Firewall and integrated IDS/IPS technology, and encapsulates in an IPSEC VPN all data replication/transit between the two Secure Enclave datacenters. The Secure Enclave 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 Secure Enclave which hosts CyberOps, 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 DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. All employees and contractors must also annually sign a DOJ Rules of Behavior 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 SP 800-53, these assessments include the management, operational, and technical controls to ensure minimization of any privacy risk.