Department of Justice
Justice Management Division

Privacy Impact Assessment
for the
Security Monitoring and Analytics Services (SMAS)

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

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

Date approved: February 16, 2023

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The U.S. Department of Justice, Justice Management Division, Office of the Chief Information Officer, Cybersecurity Service Staff (JMD OCIO CSS) developed the Security Monitoring and Analytics Service (SMAS) to provide DOJ-managed cybersecurity services to other qualified agencies requesting access to DOJ's shared cybersecurity services, referred to as "external federal agency subscribers." Consistent with the Office of Management and Budget (OMB) Memorandum M-19-16, Centralized Mission Support Capabilities for the Federal Government (April 2019), DOJ's cybersecurity services directly support the implementation of the Sharing Quality Services component of the President's Management Agenda. DOJ has been designated by the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), as the first certified federal shared service provider and Center of Excellence (COE) for Security Operations Center as a Service (SOCaaS), an OMB-designated cybersecurity shared service. SMAS capabilities include asset discovery[1], vulnerability assessment[2], Network Intrusion Detection System (NIDS)[3], Endpoint Detection and Response (EDR)[4], and Security Information and Event Management (SIEM) event correlation and log management[5]. SMAS offers JMD OCIO CSS User Behavior Analytics (UBA) and/or User Activity Monitoring (UAM) tools[6] to correlate security events in support of incident response and management.

SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity that may indicate malicious behavior and activity. DOJ provides incident information directly to the external federal agency subscriber for review and further evaluation. DOJ will only provide consulting, best practices, subject matter expertise, and guidance on incident response actions to the subscriber. DOJ does not make risk-based decisions on behalf of the external federal agency subscriber. The federal agency subscriber is responsible for remediating vulnerabilities reported to them by DOJ.

The SMAS monitors external federal agency subscriber network, system, and user activities and captures and stores files that might be related to suspicious, unauthorized, or anomalous activities. While authorized users of SMAS are limited to government employees and contractors, this Privacy Impact Assessment is necessary because SMAS might capture information and store files that contain personally identifiable information of non-governmental third-parties in connection with potential suspicious, unauthorized or anomalous activities performed on the external federal agency subscriber's networks, and systems.

---

[1] Asset discovery is the capability to identify hardware or software assets that are on the network.
[2] Vulnerability assessment is the capability to detect vulnerabilities in networks and systems that may be vulnerable to attack.
[3] NIDS is the capability to detect malicious activity by monitoring network traffic.
[4] EDR is the capability to perform on-going endpoint monitoring and analysis with the collection of endpoint data to identify, detect, and prevent advanced threats or data loss.
[5] SEIM is the capability to collect, analyze, and correlate network, user, and system data to detect anomalous activity and respond to threats.
[6] UBA and UAM are capabilities to collect, analyze, and correlate user data to find anomalous activity that may indicate a threat.

Section 2: Purpose and Use of the Information Technology

SMAS leverages JMD OCIO CSS UBA or UAM tools to cross-reference activities on external federal agency subscriber systems. SMAS has a suite of technology products, which consists of a range of commercial off the shelf (COTS) software that are customized for external federal agency subscriber use and provide insight into the subscriber's operating environment. It includes, but is not limited to:

1. Software for the ingestion and aggregation of data from a variety of sources, including endpoint security, network security, and system logs.
2. Software for the creation, tracking, and sharing of security incident data.
3. Software for performing data analytics and visualization.
4. A collaboration platform used to create, organize, and share policy, procedures, and program documents between SMAS and its external federal agency subscribers.
5. Endpoint security sensors with forensic capabilities.
6. Network security sensors with forensic capabilities.
7. Network and application scanning tools to assess for vulnerabilities within the environment.

SMAS allows DOJ to:

1. Implement and Manage Security Tools

JMD OCIO CSS implements and manages security tools including firewalls, intrusion detection and prevention technology, threat and vulnerability management tools, data loss prevention tools, filtering technologies, traffic inspection solutions, reporting technology and data analytics platforms. For JMD OCIO CSS to monitor the external federal agency subscriber's environment, communications content will be captured and retained in DOJ's information systems. JMD OCIO CSS will have access to enterprise forensic tools that support incident response investigations.

2. Investigate Suspicious Activities

With the assistance of security monitoring tools, JMD OCIO CSS analyzes alerts of suspicious activity within information systems and networks for the external federal agency subscriber. The alert provides details on a potential incident, compromise, and related threat intelligence information. JMD OCIO CSS performs triage on the alerts to understand the extent of the threat and provide appropriate responses.

If desired and procured by the external federal agency subscriber, the SMAS offering can include a tip hotline, which is a phone number where anonymous tips can be reported to JMD OCIO CSS during normal business hours. JMD OCIO CSS will use a standard call script to capture relevant information about the potential incident and share the information in a report to the external federal agency subscriber. The tips will be tracked in a limited access project set-up in JSOC's Justice Incident Management System (JIMS) or other DOJ case management system. These records will be maintained and transmitted via a secure and restricted folder in

Justice Enterprise File Sharing (JEFS),[7] limiting access to personnel with a need-to-know. The personally identifiable elements of the alerts or tips are not shared with or queried against any additional datasets outside of the data ingested for analysis or generated by the suite of technology products (the SMAS dataset). The tip reports are retained by JMD OCIO CSS for a period of one year, in accordance with applicable records schedules.

3. Reduce Downtime and Ensure Business Continuity

In the event of a breach, JMD OCIO CSS can proactively notify the appropriate stakeholders about serious security events. The system is physically located on virtual servers in the Secure Enclave,[8] as well as in external federal agency subscriber-controlled networks where endpoint agents are deployed. External federal agency subscriber data is separated from DOJ data.

4. Support Audit and Compliance

SMAS offers audit support to meet compliance requirements for government.

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

Authority		Citation/Reference
Statute	**X**	Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat 3073. The Economy Act of 1932, Ch. 314, part II, 47 Stat. 399 (codified at 31 U.S.C.1535), which authorizes agencies to enter into agreements to obtain supplies or services from another agency. DOJ Working Capital Fund (28 U.S.C. 527), establishes a working capital fund for the Department of Justice, which enables the Department to recover operational expenses for services delivered to other federal agencies.
Executive Order	**X**	Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017)
Federal Regulation		
Agreement, memorandum of understanding, or other documented arrangement	**X**	Interagency Agreement (IAA) must be executed between DOJ and external federal agency subscribers which specifies the goods

[7] JEFS is covered by separate privacy documentation. The JEFS PIA can be found at: https://www.justice.gov/jefs_pia/download.

[8] The JMD Secure Enclave is covered by separate privacy documentation. The Secure Enclave PIA can be found at: https://www.justice.gov/JMD_Secure_Enclave_PIA/download.

Authority	Citation/Reference	
		to be furnished or tasks to be accomplished by JMD OCIO CSS.
Other (summarize and provide copy of relevant portion)	**X**	OMB Memorandum M-19-02 (October 2018) OMB Memorandum M-19-16 (April 2019)

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.

The JMD OCIO CSS monitors user activities and captures and stores files that might be related to suspicious, unauthorized or anomalous activities. While monitoring the data of external federal agency subscribers, SMAS tools might capture and store files that contain personally identifiable information of non-governmental third parties connected with potential suspicious, unauthorized or anomalous activities. The information captured in this system depends on the anomalous activities detected and may vary depending on the external federal agency subscriber. It is not possible to anticipate all the situations and types of information that potentially may be captured, so we have marked all the categories below even though many of them are unlikely to be present.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	See 3.1 above
Date of birth or age	X	A, B, C and D	See 3.1 above
Place of birth	X	A, B, C and D	See 3.1 above
Gender	X	A, B, C and D	See 3.1 above
Race, ethnicity or citizenship	X	A, B, C and D	See 3.1 above
Religion	X	A, B, C and D	See 3.1 above
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	See 3.1 above
Tax Identification Number (TIN)	X	A, B, C and D	See 3.1 above
Driver's license	X	A, B, C and D	See 3.1 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: 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	X	A, B, C and D	See 3.1 above
Passport number	X	A, B, C and D	See 3.1 above
Mother's maiden name	X	A, B, C and D	See 3.1 above
Vehicle identifiers	X	A, B, C and D	See 3.1 above
Personal mailing address	X	A, B, C and D	See 3.1 above
Personal e-mail address	X	A, B, C and D	See 3.1 above
Personal phone number	X	A, B, C and D	See 3.1 above
Medical records number	X	A, B, C and D	See 3.1 above
Medical notes or other medical or health information	X	A, B, C and D	See 3.1 above
Financial account information	X	A, B, C and D	See 3.1 above
Applicant information	X	A, B, C and D	See 3.1 above
Education records	X	A, B, C and D	See 3.1 above
Military status or other information	X	A, B, C and D	See 3.1 above
Employment status, history, or similar information	X	A, B, C and D	See 3.1 above
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	See 3.1 above
Certificates	X	A, B, C and D	See 3.1 above
Legal documents	X	A, B, C and D	See 3.1 above
Device identifiers, e.g., mobile devices	X	A, B, C and D	See 3.1 above
Web uniform resource locator(s)	X	A, B, C and D	See 3.1 above
Foreign activities	X	A, B, C and D	See 3.1 above
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	See 3.1 above
Juvenile criminal records information	X	A, B, C and D	See 3.1 above
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	See 3.1 above
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	See 3.1 above
Grand jury information	X	A, B, C and D	See 3.1 above
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	See 3.1 above
Procurement/contracting records	X	A, B, C and D	See 3.1 above
Proprietary or business information	X	A, B, C and D	See 3.1 above
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	See 3.1 above
Biometric data:	X	A, B, C and D	See 3.1 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: 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
- **Photographs or photographic identifiers**	X	A, B, C and D	See 3.1 above
- **Video containing biometric data**	X	A, B, C and D	See 3.1 above
- **Fingerprints**	X	A, B, C and D	See 3.1 above
- **Palm prints**	X	A, B, C and D	See 3.1 above
- **Iris image**	X	A, B, C and D	See 3.1 above
- **Dental profile**	X	A, B, C and D	See 3.1 above
- **Voice recording/signatures**	X	A, B, C and D	See 3.1 above
- **Scars, marks, tattoos**	X	A, B, C and D	See 3.1 above
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	See 3.1 above
- **DNA profiles**	X	A, B, C and D	See 3.1 above
- **Other (specify)**	X	A, B, C and D	See 3.1 above
System admin/audit data:	X	A and B	See 3.1 above
- **User ID**	X	A and B	See 3.1 above
- **User passwords/codes**	X	A and B	See 3.1 above
- **IP address**	X	A and B	See 3.1 above
- **Date/time of access**	X	A and B	See 3.1 above
- **Queries run**	X	A and B	See 3.1 above
- **Content of files accessed/reviewed**	X	A and B	See 3.1 above
- **Contents of files**	X	A and B	See 3.1 above
Other (please list the type of info and describe as completely as possible):			

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone	X	Email	X		
Other (specify): SMAS enables the identification and evaluation of suspicious, unauthorized or anomalous activity that may indicate malicious behavior and activity. Individuals will directly provide, or systems will automatically collect, user profile information, contact information, and other personally identifiable information (PII) necessary and relevant to the respective tools, services, and applications.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal Entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): DOJ provides external federal agency subscribers with the technical capability to protect their data from malicious or accidental threats. SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity that may indicate malicious behavior and activity. Government sources will directly provide, or systems will automatically collect, user profile information, contact information, and other PII necessary and relevant to the respective tools, services, and applications. Because external federal agency subscribers may be communicating and interacting with entities both within and outside the United States Government that would be subject to monitoring by SMAS, the source of the records captured with SMAS may come from any of the sources selected above.					

Non-government sources:					
Members of the public		Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): The tools, services, and/or applications utilized by SMAS may capture, audit, and log information from private-sector service vendors, and citizens that access the external federal agency subscriber's network, system, and application. Because external federal agency subscribers may be communicating and interacting with entities both within and outside the United States Government that would be subject to monitoring by SMAS, the source of the records captured with SMAS may come from any of the sources selected above.					

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.

JSOC will provide the external federal agency subscriber point of contact with relevant information via secure means of communication. The data shared with the external federal agency subscriber consists of report(s) on the automated alerts generated by the tools or manually collected through the hotline. At the request of the external federal agency subscriber, JMD OCIO CSS can provide custom reports, which may be grouped by username, host name, IP address or another key indicator. The personally identifiable elements of the alerts or tips are not shared with or queried against any additional datasets outside of the datasets collected by SMAS. At the request of the external federal

agency subscriber, JSOC can provide custom reports from the SMAS dataset.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	**X**		**X**	JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared within the component on a case-by-case basis (for example, as part of incident response efforts).
DOJ Components	**X**			JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared with DOJ components on a case-by-case basis (for example, as part of incident response efforts).
Federal entities	**X**			JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared with federal entities on a case-by-case basis (for example, as part of incident response efforts).
State, local, tribal gov't entities	**X**			JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared with State, local, tribal gov't entities on a case-by-case basis (for example, as part of incident response efforts).
Public				N/A

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	**X**			JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared with counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes on a case-by-case basis (for example, as part of incident response efforts).
Private sector	**X**			JMD OCIO CSS looks into suspicious activity within IT systems and networks. Information may be shared with DOJ's private sector service vendors, on a case--specific basis, for system administration, including but not limited to, tool, service, and/or application troubleshooting.
Foreign governments				N/A
Foreign entities				N/A
Other (specify):				N/A

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.

The data SMAS collects 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.

DOJ users have been constructively notified that DOJ collects, uses, maintains, and discloses account, audit log, and user records in SMAS, by publishing DOJ's System of Records Notice, JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (July 14, 2021).

Individuals are also constructively informed about the collection, use, sharing or other processing of their records within SMAS, via JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 FR 41089 (7-30-2021), providing generalized notice 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.

SMAS enables the identification and evaluation of suspicious, unauthorized, or anomalous activity that may indicate malicious behavior and activity. Individuals will not be provided an opportunity to voluntarily participate in the collection, use, or dissemination of information provided to the JMD OCIO CSS through SMAS.

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.

As stated above, individuals have been constructively notified that the DOJ maintains records in SMAS by DOJ's publication of JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" 86 FR 37188 (July 14, 2021) and JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, 86 FR 41089 (7-30-2021). Both SORNs detail the process by which a person can access records pertaining to that individual, or amend records that the individual believes are inaccurate, irrelevant, untimely, or incomplete, subject to applicable exemptions.

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):** **The SMAS leverages existing DOJ authorized information systems to deliver services to the federal agency subscribers. The following authorized systems are:** • Secure Enclave, Ongoing Authorization • JUTNet, 5/12/2020 • Cyber Operations, 7/13/2021 • Logging as a Service, 10/22/2020
	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:** SMAS has a suite of technology products which consists of a range of COTS software that are required to undergo an initial authorization to operate, followed by continuous monitoring of security controls. At a minimum, the SMAS tools require monthly vulnerability and configuration scans.
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:** At a minimum, audit logs are reviewed weekly.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** All DOJ users must complete computer security awareness training annually, as well as read and agree to comply with DOJ information technology Rules of Behavior both prior to accessing the DOJ network, and annually thereafter. DOJ 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 complete security control assessment has been completed for the systems that support SMAS, to include physical and logical access, identification and authentication, vulnerability management, auditing, and other assessment actions to ensure that security controls are

operating as intended. JMD makes use of separate Privileged and Non-Privileged user accounts and leverages additional role-based access control technologies and administrator session recording. All system and application log data is being sent to JMD's centralized audit log management system for triage and review.

Because SMAS will be maintained within the DOJ Secure Enclave, SMAS will also utilize the technical safeguards implemented within Secure Enclave. For example, SMAS tools uses Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2,[9] to protect data in transit between the browser and the user's workstation, makes use of Application Layer Firewall[10] and integrated Intrusion Detection System / Intrusion Prevention System[11] technology, and encapsulates in an Internet Protocol Security Virtual Private Network (IPSEC VPN)[12] all data replication/transit between the two Secure Enclave data centers. The Information Security System Officers (ISSOs) are charged with reviewing logins and performing auditing functions to ensure role-based access controls satisfy 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: Information Systems Security Records, Transmittal No. 26 September 2016, item 010–062 and General Records Schedule 5.6: Security Records, Transmittal No. 31 April 2020, item 210–240, 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.

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

---

[9] NIST FIPS 140-2 can be found at: https://csrc.nist.gov/groups/STM/cmvp/standards.html.
[10] An "Application Layer" firewall is a form of firewall that controls input, output, and/or access from, to or by an application or service.
[11] 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.
[12] 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.

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 users' account, audit log, and user records are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records," 86 FR 37188 (July 14, 2021).

JUSTICE/JMD-026, Security Monitoring and Analytics Service Records, to cover all other SMAS records. Members of the public can access JUSTICE/JMD-026 on the DOJ SORN webpage: https://www.justice.gov/opcl/doj-systems-records.

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.***

JMD utilizes tools, services, and applications that may collect PII, and those systems may collect other sensitive systems operation information to include names, personal e-mail addresses, personal phone numbers, device identifiers, and system admin/audit data (e.g., user IDs, user passwords, IP addresses, date/time of actions, queries run, and contents of files). JMD's collection and use of PII, as described here and throughout this PIA, may create certain privacy risks such as potential unauthorized access to and disclosure of PII information through a system compromise. To mitigate these risks, records are managed in accordance with applicable federal records retention schedules.

Additionally, 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 where applications hosted on the Secure Enclave are offered as a service. To further mitigate any risks associated with these activities, the Secure Enclave implements encryption, account management and access controls, auditing, and system monitoring tools to protect PII. JMD makes use of separate Privileged and Non-Privileged user accounts and access is granted

based on least privilege and need-to-know requirements. DOJ non-privileged users (government and contractors) will not have access to the collection, use, or dissemination of information obtained through SMAS.

To further mitigate any risks, such as unauthorized access to and disclosure of PII through a system compromise associated with these activities, the SMAS tools uses encryption and logging controls for mitigation purposes. The Secure Enclave which host the SMAS tools makes use of Secure Sockets Layer (SSL) 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, 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 data centers. ISSO(s) perform(s) continuous monitoring of the security controls within the system to ensure security protections are operating as intended.

By Department Order, all DOJ users (federal and contractor) with access to Department networks, must complete annual Cyber Security Awareness Training (CSAT). 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 agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training can result in termination of the employee or contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training. Finally, 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.