Criminal Division

Privacy Impact Assessment
for the
MLARS Statistical Analysis System (MSAS)

Issued by:
Jennifer A.H. Hodge
Criminal Division, Senior Component Official for Privacy

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

Date approved: [June 6, 2023]

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

The United States Department of Justice (DOJ or Department), Criminal Division (CRM or Division), Money Laundering and Asset Recovery Section (MLARS), Special Financial Investigations Unit (SFIU) and its partner law enforcement agencies pursue the most sophisticated money laundering cases and investigations, including violations related to the International Emergency Economic Powers Act (IEEPA),[1] the Trading with the Enemy Act (TWEA),[2] and the Bank Secrecy Act (BSA).[3] The challenges MLARS faces include determining: the scope of financial activity involved in a scheme; the specific intent of criminal or foreign organizations and senior corporate officers who intentionally violate criminal financial institution and money laundering statutes; or who pose a threat to the national security, foreign policy, or economy of the United States. Therefore, MLARS is standing up the MLARS Special Analytics System (MSAS).

MSAS is a sophisticated and specialized financial investigative tool that allows investigators and prosecutors to analyze disparate, complex data for patterns and inconsistencies indicating criminal activity. MSAS will also allow for the forensic tracing of criminal proceeds and facilitation of funds through different international jurisdictions, ultimately leading to their seizure by the U.S. Government.

The Division conducted this Privacy Impact Assessment (PIA) to assess and mitigate the risks to the personally identifiable information (PII) collected in this system, which includes but is not limited to names, contact information, Social Security Numbers (SSNs) and financial 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.

MLARS and its investigative partners occasionally encounter urgent and complex financial investigative needs which strain the support capabilities of the existing CRM Information Technology Management Section (IT). While the Department has a substantial investment in tools to support routine investigations, the challenges in unique cases and investigations involving violations related to the IEEPA, the TWEA, and the BSA invariably involve in-depth relationship, financial, and metadata analysis. Therefore, MLARS requires sophisticated and specialized IT tools and support to load, organize, assimilate, and summarize data and information related to financial institutions, third party money launderers, kleptocrats, and other targets actively pursued by the SFIU.

To successfully conduct SFIU's complex investigations, millions of records often need to be

---

[1] *See* https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim
[2] *See* https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter35&edition=prelim
[3] *See* https://home.treasury.gov/system/files/126/ieepa.pdf

reviewed, and the content of those records must be analyzed to identify relationships between the decisions or actions of the subjects of investigations and specific financial transactions. The records may have different formats, come from different places, and may include foreign languages. Examples include, but are not limited to, corporate accounting and finance records, bank account records, domestic and international financial transaction records, BSA filings (such as Suspicious Activity Reports), internal corporate e-mails, corporate minutes, corporate organization charts, corporate policy documents, customer sales records including account documents, and personnel records including performance evaluations.

MSAS analyzes law enforcement sensitive materials, as well as subpoenaed documents protected by the Federal Rules of Criminal Procedure.[4] The documents will consist primarily of financial records, books, ledgers, and bank account statements that will be used as evidence in Federal criminal prosecutions for money laundering, bank fraud, wire fraud, Racketeer Influenced and Corrupt Organizations (RICO),[5] and violations of IEEPA. MSAS will allow investigators and prosecutors to analyze disparate, complex data for patterns and inconsistencies indicating criminal activity. MSAS will also allow for the forensic tracing of criminal proceeds and facilitation of funds through different international jurisdictions, ultimately leading to their seizure by the government.

Some examples of the analytical functions performed by MSAS include:

- Identifying and tracing funds through banks, offshore shell companies, hawalas, and other financial entities;
- Automatic tracing of wire transfers using trace numbers or monetary amounts of the transfers;
- Providing graphic depictions, spreadsheets, and link analysis of the institutions which funds passed through, the individuals who sent and received the funds, and confirmation of the correct monetary amounts;
- Incorporating the information learned by investigators on a subject or entities' standard practices or other investigative information;
- Ingesting and searching emails for instructions on financial transactions and matching them to corresponding transactions based on monetary amount, dates, transactions, or other elements;
- Stitching together information from multiple sources;
- Performing a variety of searches;
- Performing reactive and proactive analysis;
- Performing link analysis and create link charts;
- Performing timing series analysis;
- Performing geospatial analysis of events, transactions, subjects of investigation, and business entities;
- Creating data summaries;
- Analyzing communication and cryptocurrency transfer data;
- Identifying sources and destinations of funds;

---

[4] *See* https://www.federalrulesofcriminalprocedure.org/
[5] *See* https://www.justice.gov/archives/jm/criminal-resource-manual-109-rico-charges

- Identifying various money laundering techniques such as structuring, layering, and passthrough accounts;
- Analyzing text content and documents in order to identify and extract content that matches a specific pattern and identify documents or text blocks which are similar, and automatically identifying and extracting entities from text ("entity extraction"); and
- Incorporating other public source information such as social media, public records data, social media data, website content, and other open-source information.

MSAS does not create an independent system of records but serves to analyze records and information that are already or will be incorporated into Division investigative case files.

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	18 U.S.C. § 3001 *et seq.*; Asset Forfeiture and Money Laundering Statutes;[6] 28 U.S.C. § 516. Conduct of litigation reserved to Department of Justice; 28 U.S.C. § 519. Supervision of litigation; 28 U.S.C. § 510. Delegation of authority; 18 U.S.C. §§ 1956 and 1957
☐ Executive Order	
☒ Federal Regulation	28 C.F.R. part 0, subpart K—Criminal Division; 28 C.F.R. § 0.55 - General functions (Criminal Division)
☒ Memorandum of Understanding/agreement	The Attorney General's Guidelines on the Asset Forfeiture Program, July 2018;[7]
☒ Justice Manual[8]	Title 9, Criminal; 9-105, 111-121
☐ Other (summarize and provide copy of relevant portion)	

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 information in MSAS depends on the data provided to the Division for each specific case.

---

[6] *See* https://www.justice.gov/criminal-mlars/file/1146911/download
[7] *See* https://www.justice.gov/criminal-mlars/file/1123146/download
[8] *See* https://www.justice.gov/jm/justice-manual

Given the varied nature of the Division's work, the data entered into MSAS could include any type of information included in the chart below for any U.S. or non-U.S. Person, as they appear in lawfully obtained investigative records unless otherwise indicated in the comments section.

(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	Also includes government personnel for account access management purposes.
Date of birth or age	X	C & D	
Place of birth	X	C & D	
Gender	X	C & D	
Race, ethnicity or citizenship	X	C & D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	
Tax Identification Number (TIN)	X	C & D	
Driver's license	X	C & D	
Alien registration number	X	C & D	
Passport number	X	C & D	
Mother's maiden name	X	C & D	
Vehicle identifiers	X	C & D	
Personal mailing address	X	C & D	
Personal e-mail address	X	C & D	
Personal phone number	X	C & D	
Professional mailing address	X	C & D	
Professional e-mail address	X	A, B, C & D	Also includes government personnel for account access management purposes.
Professional phone number	X	C & D	
Professional title	X	C & D	
Medical records number	X	C & D	
Medical notes or other medical or health information	X	C & D	
Financial account information	X	C & D	
Applicant information	X	C & D	
Education records	X	C & D	
Military status or other information	X	C & D	

(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
Employment status, history, or similar information	X	C & D	
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C & D	
Certificates	X	C & D	
Legal documents	X	C & D	
Device identifiers, e.g., mobile devices	X	C & D	
Web uniform resource locator(s)	X	C & D	
Foreign activities	X	C & D	
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C & D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	C & D	
Whistleblower, e.g., tip, complaint or referral	X	C & D	
Grand jury information	X	C & D	
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C & D	
Procurement/contracting records	X	C & D	
Proprietary or business information	X	C & D	
Metadata from emails, electronic communications, social media or other documents	X	C & D	
Location information, including continuous or intermittent location tracking capabilities	X	C & D	Includes potential locations of individuals, as reflected by financial transactions or metadata associated with electronic records. MSAS will not be used to "geo-track" individuals over time.
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			

(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
- **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:			
- **User ID**	x	A	
- **User passwords/codes**			
- **IP address**	x	A	
- **Date/time of access**	x	A	
- **Queries run**	x	A	
- **Content of files accessed/reviewed**	x	A	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B, C & D	Given the varied nature of the Division's work, the information placed into MSAS could include any type of lawfully obtained, unclassified information reasonably determined by the Department to be necessary and/or relevant to a law enforcement investigation.

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

Directly from individual about whom the information pertains		
☒ In person	☒ Hard copy: mail/fax	☒ Online
☒ Telephone	☒ Email	
☒ Other (specify):	Information could be obtained from the individual's counsel, through the investigative interview processes, or via the pre-trial discovery processes, which could be conducted in any format highlighted under this category.	
Government sources		
☒ Within the Component	☒ Other DOJ components	☒ Other federal entities
☒ State, local, tribal	☒ Foreign	

☐ Other (specify):		
Non-government sources		
☒ Members of the public	☒ Public media, internet	☒ Private sector
☒ Commercial data brokers		
☒ Other (specify):	Information could be obtained from legal processes including subpoenas and search warrants or from accessing publicly available information.	

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	☒	☐	☐	Information will be shared on a case-case basis with law enforcement and prosecutorial entities involved in the investigation and prosecution and who have a need-to-know. It will be shared with counsel, parties, witnesses, and courts through the discovery process on a case-by-case basis, or through judicial hearings. Some records filed in court may be publicly available pursuant to court rules.
DOJ Components	☒	☐	☐	
Federal entities	☒	☐	☐	
State, local, tribal gov't entities	☒	☐	☐	
Public	☐	☐	☐	
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	☒	☐	☐	
Private sector	☐	☐	☐	
Foreign governments	☒	☐	☐	
Foreign entities	☐	☐	☐	
Other (specify):	☒	☐	☐	Information may be contained within reports to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, and resource requests.

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.

This information will not be released to the public for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Individuals are provided with general notice of the existence of case files through Division SORN CRM-001, Central Criminal Division Index File and Associated Records last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007) and amended at 82 Fed. Reg. 24155 (May 25, 2017).

Individuals are provided with general notice of Department of Justice computer systems access and activity records through Department SORN DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, last published in full at 86 Fed. Reg. 37188 (Jul. 14, 2021).

In instances where a prosecution occurs, individuals and their counsel will be provided with the relevant information from MSAS through the Federal criminal or civil discovery process.

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.

Generally, subjects and targets of investigations are not provided the opportunity to voluntarily participate in the collection, use or dissemination of information in the system, as such notice and opportunity may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation.

However, in certain circumstances, information in MSAS could be collected directly from interviews of investigative subjects or their counsel, which may give such individuals notice of collection though potentially not the opportunity for voluntary participation.

DOJ users operating the system do not have the opportunity to consent to particular uses of the information nor decline to provide information. DOJ employees are presented with the opportunity to acknowledge the collection of their information when accessing the system.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Individuals who are the subject of records contained in CRM investigative, or litigation case files covered by the JUSTICE/CRM-001 SORN will not be provided with Privacy Act access

or amendment capabilities to the records in MSAS, as doing so may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation. Information in this system is exempt from the access, amendment, correction, and notification procedures of the Privacy Act.[9]

In instances where a prosecution occurs, defendants are afforded access to information in this system about them pursuant to the Federal Rules of Criminal and Civil Discovery.[10] Disagreements regarding the content of information would be addressed during pre-trial or trial proceedings.

Although exemptions may apply, individuals, including users of the system, seeking to gain access to information within JUSTICE/CRM-001 may request amendment or correction of their respective information, and/or receive notification of the procedures, by making a Freedom of Information Act (FOIA) and/or Privacy Act of 1974 request by following the provisions of those statutes and DOJ regulations on those statutes. Such requests will be processed according to the provisions of the FOIA.

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):** July 12, 2023 **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:** All ATO process and risk assessment materials, including the existence of POAMs resulting from those processes are recorded in the Justice Management Division's (JMD) Cyber Security Assessment and Management (CSAM) tool. This information is normally considered Information System Vulnerability Information and is controlled by the relevant Information System Security Officer.

[9] As relates to JUSTICE/CRM-001, exemptions are claimed pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). *See* 28 C.F.R. § 16.91. As relates to JUSTICE/DOJ-002, exemptions are claimed pursuant to 5 U.S.C. 552a (k)(1) and (k)(2). *See* 86 FR 61687.

[10] For more information on the Federal Rules of Criminal Discovery, *see* https://www.federalrulesofcriminalprocedure.org/. For more information on the Federal Rules of Civil Discovery, *see* https://www.federalrulesofcivilprocedure.org/.

	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:** MSAS undergoes continuous assessments, penetration tests, and vulnerability scans, and is monitored through the CRM IT Security Continuous Monitoring Program. CRM performs vulnerability and configuration management scanning using both tools provided by the DOJ Office of the Chief Information Officer and provided by CRM IT. Continuous monitoring includes the security assessment process; and a manual review audit occurs at regular intervals, to the extent required by the National Institute of Standards and Technology special publication (SP) 800-53.[11]
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:** The Division collects logs according to the standards in the DOJ Cybersecurity Standards, which include Operating System, Web, Database and Application logs for this system. Logs are correlated into appropriate DOJ information systems managed by JMD. Access to these logs is provided to the Justice Security Operations Center, who provided security analysis and log monitoring for unusual activity to the extent required by NIST SP 800-53. Information Owners and Stewards that identify additional audit review requirements per the NIST control selections in their System Security Plan, and further defined by entries in a Continuous Monitoring Implementation Plan (CRM Template), may have reports designed to monitor for unusual activity. These reports would be reviewed on the basis determined by the information owner.
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:** One-on-one training, specific to this system, is conducted for authorized users. Training videos and manuals are also available for the users' personal reference.

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?

[11] *See* https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/archive/2015-01-22.

All Division systems implement technical security to reduce the risk of compromise to PII information. Specifically, certain access and security controls have been utilized to protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- MSAS has a security categorization of "Moderate-impact" and has selected the applicable security controls for a Moderate baseline.[12] The Division will ensure that MSAS only solicits information categorized as Medium- or Low-Impact under NIST FIPS Publication 199 and NIST SP 800-60, Volume II publications and that no data fields solicit "High-impact" information without specifically granted approval from appropriate privacy and security personnel, to ensure adequate controls are applied to protect such information.[13]
- The system is accessible by DOJ employees and contractors only and utilizes "tiered" or role-based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified through the staff's PIV card.
- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- As described throughout this PIA, all MSAS users must complete the Department's annual Cyber Security and Awareness Training (CSAT), as well as read and agree to comply with DOJ's Information Technology and Privacy Rules of Behavior. MSAS system administrators must complete additional professional training, which includes security training.
- Audit logging is configured, and logs are maintained to help ensure compliance with tiered access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, MSAS's defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

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.)

---

[12] Per NIST SP 800-60, Vol. II, a Moderate-impact system is one in which the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals, *see* https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-60v2r1.pdf.

[13] Per NIST SP 800-60, Vol. II, a High-impact system is on in which the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals, *see* Id.

Disposition of records within MSAS will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of hardcopy and softcopy records.

Records will be retained or disposed of pursuant to National Archives and Records Administration (NARA) retention schedules N1-060-88-10 and N1-060-93-13. Upon approval by NARA, the retention schedules will be replaced with DAA-0060-2021-0001.

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. ☒ 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:

- Records related to CRM correspondence, cases, matters and memoranda, including but not limited to, investigative reports, correspondence to and from CRM, legal papers, evidence, and exhibits, used to provide investigative and litigation information to management in CRM and the Department, courts, and other law enforcement agencies are covered by System of Records Notice JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007 and amended at 82 Fed. Reg. 24155 (May 25, 2017).
- User accounts, records and audit logs maintained in this system to monitor system activity are covered by System of Records Notice 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 (Jul. 14, 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?

Privacy Risk: Unauthorized Access or Misuse of Information

Mitigation: DOJ employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. MSAS also implements access monitoring, privacy and records controls standardized by the National Institute of Standards and Technology Security and Privacy Controls for Federal Information Systems, as defined in NIST Special Publication 800-53.

Access to this system is limited based on a need-to-know, and further limited to the minimum access needed. Access is granted to SFIU personnel on a case-by-case basis which limits personnel to only those cases on which they work. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's Personal Identity Verification (PIV) card and PIN number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by the Federal Information Security Modernization Act of 2014 (FISMA). An audit log is maintained of all user logins and certain user actions such as queries run, and files accessed or reviewed. Notification of the monitoring is presented clearly when logging into the system.

Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's Cyber Security and Awareness Training (CSAT), as well as read and agree to comply with DOJ Information Technology and Privacy Rules of Behavior. This occurs during their orientation upon entering into service with DOJ, and annually thereafter. MLARS provides one-on-one training for employees granted access to MSAS. The Division maintains an Account Management Guide and Configuration Management Guide for MSAS, which users may reference for additional technical support.

The IT system assessment is documented in the DOJ CSAM tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no access to this system by personnel not assigned to SFIU; administrator access is restricted to the few DOJ employees and contractors who administer the program.

Privacy Risk: Name Association with a Criminal Investigation

Mitigation: As in most cases where a record associates a person with a criminal investigation, the mere presence of a name in the system can generate the assumption of involvement with criminal activity or other damage to their reputation. For this reason, there is no automated dissemination of information from this system outside of the Division. Any dissemination must be done pursuant to proper authority and management review. Information obtained from this system is considered law enforcement sensitive. Additionally, in all instances possible, PII will be removed from any reports that are generated for management.

Privacy Risk: Over-Collection of Information

Mitigation: Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. Due to the sophistication and expanse of the criminal enterprises investigated by SFIU, the information needed to discern the entire scope of the activity can be more extensive than less sophisticated cases.

This system stitches together all information provided and uses a series of calculations to determine patterns or relevant links. The Division relies on a two-step approach to mitigating overcollection concerns. The first involves the selection of included information. The

information collected in MSAS is that contained in the official investigative case file. Thus, it must be lawfully obtained, unclassified information reasonably determined to be necessary and/or relevant to a law enforcement investigation. All information is collected by law enforcement, analysts, and attorneys trained in the application of the Federal Rules of Criminal and Civil Procedures to determine whether information is relevant and appropriate. In passing this bar, all information available from the case file will be appropriate for enhanced analysis in MSAS.

The second prong relies on the extensive training and cumulative experience of the specialized and expert financial investigators, analysts, and prosecutors to further tailor the most appropriate case file information for entry in MSAS. SFIU personnel are the subject-matter experts who specialize in these sophisticated financial investigations and have extensive and cumulative knowledge of the types of information most relevant and pertinent to their investigations. Their operation of MSAS according to their knowledge, experience, and training, serves as a gatekeeper to appropriately control the content entered into the system.

Privacy Risk: Erroneous or Inaccurate Information

Mitigation: Based on the sensitive investigative nature of these records, members of the public cannot enter records directly into the system or access it for review. Information in this system is obtained through investigative agencies and prosecutorial or court documents. DOJ has a substantial interest in ensuring the accuracy of the information in this system and integrity of information that is, or may become, evidence. Both the investigating agencies and DOJ verify this information as part of the normal procedures associated with day-to-day tasks, which include multiple levels of oversight and review, and adherence to court rules concerning evidence. Every effort is made to diligently review, verify, and correct information from these records, while maintaining the integrity of evidence. Investigations and prosecutions are conducted in the timeliest manner possible based on the variables and complexities of each case.