

Drug Enforcement Administration



Privacy Impact Assessment for the Digital Evidence Laboratory Findings Network (SFL9FN)

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Kameron Cox
Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: September 21, 2026

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

Throughout the course of a lawful investigation, Drug Enforcement Administration (DEA) investigators may obtain digital evidence in the form of an electronic device and its associated data. Seized electronic evidence may take many different forms – mobile phones, tablets, laptop computers, desktop computers, servers, DVRs, etc. The Digital Evidence Laboratory extracts electronic evidence from electronic devices, seized via warrant or other legal process by DEA case agents in criminal investigations, and provides it to DEA investigators.

The Digital Evidence Laboratory Findings Network (SFL9FN) is designed to allow Digital Evidence Laboratory (SFL9) staff to conduct forensic examinations to extract electronic evidence from electronic devices. Additionally, the SFL9FN system also allows the DEA case agents/analysts in the investigative case team to review digital evidence work product of the SFL9 staff through a secure connection within the internal DEA network.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The purpose of the SFL9FN system is to allow digital forensic examiners to conduct forensic examinations on lawfully obtained electronic devices containing digital evidence, create findings, and provide a review platform for case investigators. DEA Special Agents collect electronic devices in the course of their investigations, which may include computer hard drives, thumb drives, cell phones, and any other data storage devices. The digital evidence is lawfully collected via warrant or other legal process as part of DEA investigations for criminal and civil law enforcement purposes. The devices may contain a variety of categories of personally identifiable information (PII).

DEA uses various electronic tools to access, extract, analyze and organize this information so that it may be searched and used for investigatory purposes. The purpose of the electronic tools used is to sift through large amounts of information in response to the search warrant and user inquiries or programmed functions to produce results that may be analytically useful in connection with an investigation or other law enforcement activity. For instance, these tools may look for known names, addresses, cellphone or landline numbers, credit card information, specific record types, or a specific string of words or numbers, among other things. The search will be customized depending on what is needed to support an investigation. Special Agents and analysts develop search strings and other queries to apply to the digital devices in order to produce a relevant result.

The Digital Evidence Laboratory maintains a comprehensive and evolving inventory of forensic tools to support laboratory operations. These tools are selected to address both general forensic analysis requirements and specific investigative needs. Some tools can be used to highlight anomalies in the data, but are not used for “data mining” as that term is defined by law, as data from each case is placed in silos to limit searching across cases, thereby ensuring inputs are associated with a specific individual or group of individuals.¹ As technology advances and new hardware or software applications emerge, the laboratory regularly acquires new tools for unique or single-use scenarios. Given the dynamic nature of this inventory, it is impractical to provide an exhaustive list of all tools in use. Relatedly, DEA uses the physical, technical, and administrative protections in place within the SFL9FN system and the lab at large, as opposed to each individual tool, to ensure individual privacy and data protection at the laboratory. This assessment categorizes forensic tools used by the lab according to their primary functions and applications to provide transparency to the potential impacts to individual privacy, and analyzes SFL9FN and the laboratory’s safeguards to mitigate such impacts. It is important to note that forensic tools may serve multiple functions across these categories or may be specialized for a single aspect of the forensic process.

Categories of Forensic Tools

1. Access Tools

Access tools are designed to facilitate entry to physical evidence or digital applications. These may include drivers that enable communication between forensic workstations and hardware, applications that interface with forensic devices, or tools that bypass security measures on physical devices or software. The primary objective of access tools is to obtain data from seized devices for further examination. Various tools can be used to produce different results. For instance, one tool might display an index where relevant search terms are found in seized devices and another tool might extract data from deleted files or hidden partitions.

2. Preservation Tools

Preservation tools are responsible for collecting digital evidence from seized devices in a manner that ensures the integrity and completeness of the data. This typically involves creating bit-for-bit copies of digital information while safeguarding it from alteration, deletion, or corruption. The preservation process is critical to maintaining the admissibility of evidence in judicial proceedings. Tools in this category may oversee the entire preservation process or specific aspects thereof.

3. Decoding Tools

Decoding tools convert raw, machine-readable data into formats that are accessible and interpretable by forensic examiners. This translation can occur at various levels, including files, folders, or entire file systems. Decoding is essential for enabling subsequent analysis and review.

4. Analysis Tools

Analysis tools support the systematic evaluation of preserved and decoded digital evidence. These tools enable examiners to reconstruct events, correlate information, and identify relevant facts. The analysis process is structured to ensure evidence integrity and to facilitate the presentation of findings in legal contexts.

¹ See 42 USC § 2000ee-3(b)(1)

5. Presentation Tools

Presentation tools assist in communicating the results of forensic analysis to stakeholders, including case agents, investigators, and the courts. These tools are used to transfer knowledge and findings in a clear and accessible manner.

Access to SFL9FN is extremely limited. The network has no connections to the internet and only has a single connection to DEA's internal network. This connection also has a firewall that limits communication between the networks. The network only exists within DEA facilities behind physical security; there is no mobile device access to any information in SFL9FN. Chain of custody and access to the evidence is tracked. Access to individual electronic case files stored within SFL9FN is limited to those authorized laboratory personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file.

After an exhibit is submitted to the lab pursuant to legal process, DEA case agents are provided access to data present on the exhibit through a virtual machine / remote desktop connection accessible from within DEA's internal network. Access is limited to a standard period of time. Once the agent's account expires and it is not renewed, the Virtual Machine (VM) is taken off-line. The case agent(s) can only view content and do not have the ability to download files, print files, or have direct access to the evidence. The Agent identifies relevant data in accordance with the purpose of the seizure and DEA's legal authority by tagging the record. As no one outside the lab may copy contents, the lab uses the agent's tags to conduct a follow-up forensic examination and create any necessary supplementary reports. The final work products of the laboratory (outside of the SFL9FN network), which include complete archives of the evidence and examiner reports, are contained in portable hard drives or Blu-ray discs and are mailed to the case agent via controlled carrier.

The results of the findings are used to further DEA investigations and selectively for presentation in court.

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	21 U.S.C. § 801 <i>et seq.</i> , (see specifically 21 U.S.C. §§ 878-880). Controlled Substances Act 44 U.S.C. § 3101 – Authority to Make Records of Agency Processes.
Executive Order	
Federal regulation	28 C.F.R. §§ 0.100 and 0.101
Agreement, memorandum of understanding, or other documented arrangement	
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.*

(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
<i>Example: Personal email address</i>	X	B, C and D	Email addresses of members of the public (US and non-USPERs)
Name	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Date of birth or age	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Place of birth	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Gender	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Race, ethnicity, or citizenship	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Religion	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Tax Identification Number (TIN)	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Driver's license	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Alien registration number	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Passport number	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).

(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
Mother's maiden name	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Vehicle identifiers	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Personal mailing address	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Personal e-mail address	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Personal phone number	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Medical records number	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Medical notes or other medical or health information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Financial account information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Applicant information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Education records	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Military status or other information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Employment status, history, or similar information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Employment performance ratings or other performance information, e.g., performance improvement plan	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Certificates	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Legal documents	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Device identifiers, e.g., mobile devices	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).

(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
Web uniform resource locator(s)	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Foreign activities	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Juvenile criminal records information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Procurement/contracting records	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Proprietary or business information	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
Location information, including continuous or intermittent location tracking capabilities	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
<i>Biometric data:</i>			
- Photographs or photographic identifiers	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
- Video containing biometric data	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER).

(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 Detainees; 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
- Scars, marks, tattoos			
- Vascular scan, e.g., palm or finger vein biometric data			
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID	X	A	System admins and/or audit functions collect such information for DEA employees conducting analysis;
- User passwords/codes	X	A	System admins and/or audit functions collect such information for DEA employees conducting analysis; Unstructured data may contain this type of information for members of the public (US and Non-USPER).
- IP address	X	A	System admins and/or audit functions collect such information for DEA employees conducting analysis; Unstructured data may contain this type of information for members of the public (US and Non-USPER).
- Date/time of access	X	A	System admins and/or audit functions collect such information for DEA employees conducting analysis; Unstructured data may contain this type of information for members of the public (US and Non-USPER).
- Queries run			
- Contents of files	X	C and D	Seized evidentiary data may contain this type of information for members of the public (US and Non-USPER)-
Other (please list the type of info and describe as completely as possible):	X	C and D	Unstructured data may contain User IDs, User Passwords/Codes; IP addresses, Date/time of access, and contents of files information from seized devices for members of the public (US and Non-USPER). Virtually any kind of PII could be stored on such devices.

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	(Search Warrant Return) Online	X

Phone	X	(Search Warrant Return) Email	X	(Search Warrant Return) Seized Device	X
Other (specify): Note: Digital Evidence information originates from the devices (i.e., evidence hardware such as laptops, desktops, mobile phones, remote content, etc.) that are obtained from the user or owner of the device in the course of DEA investigation, pursuant to legal authorization, such as a search warrant. The DEA investigator provides the device(s) to the Digital Evidence Laboratory and requests forensic imaging and analysis.					

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): Note: Digital Evidence information originates from the devices (i.e., evidence hardware such as laptops, desktops, mobile phones, remote content etc.) that are obtained from the user or owner of the device in the course of a DEA investigation, pursuant to legal authorization, such as a search warrant. The DEA investigator provides the device(s) to the Digital Evidence Laboratory and requests forensic imaging and analysis. Information may be obtained from other DOJ components, other Federal entities, or State, local, tribal government entities and foreign sources s by DEA as it relates to a specific investigation.					

Non-government sources:					
Members of the public	X	Public media, Internet		Private sector	X
Commercial data brokers					
Other (specify): Note: Digital Evidence information originates from the devices (i.e., evidence hardware such as laptops, desktops, mobile phones, remote content etc.) that are obtained from the user or owner of the device in the course of a DEA investigation, pursuant to legal authorization, such as a search warrant. The DEA investigator provides the device(s) to the Digital Evidence Laboratory and requests forensic imaging and analysis. Information could be volunteered by member of the public or provided by private sector as part of a legal search warrant.					

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	Access is only granted to individual laboratory examiners performing the work (DEA employee / contractors) while the DEA investigative team has read only access to a subset of the data and the final report. All other DEA users do not have access.
DOJ Components	X			Information sharing within DOJ is limited to DOJ officers and employees who have a legitimate need for the record in the performance of their duties. Information in this system may be shared with U.S. Attorneys in relevant operations/ prosecutions/ cases. Data may be shared, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation. However, the lab does not share data external to DEA.
Federal entities	X			DEA may share data, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation. However, the lab does not share data external to DEA. All data shared from SFL9FN is shared via external devices sent to the case agent or

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.
				Chief Counsel's office, who do not have access to SFL9FN. Only specific DEA users authorized to have access to SFL9FN have such access.
State, local, tribal gov't entities	X			DEA may share data, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation. However, the lab does not share data external to DEA. All data shared from SFL9FN is shared via external devices sent to the case agent or Chief Counsel's office, who do not have access to SFL9FN.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Material may be disclosed in the course of criminal or civil discovery. The listed recipient parties DO NOT have direct access to the system.
Private sector				
Foreign governments	X			Evidence may be received from foreign law enforcement partners. Data can be shared with foreign law enforcement partners on a case-specific basis once the data leaves the network. These foreign law enforcement partners DO NOT have access to SFL9FN.
Foreign entities				
Other (specify):				

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.

Information is not directly released to the public.

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.*

Notification is provided to individual from whom the device is retrieved at the time of collection by execution of the search warrant. Information may also be provided by written consent. The information being sought is detailed within the search warrant or consent. Information in SFL9FN is covered by the DEA SORN, Justice/DEA-008, Investigative Reporting and Filing System, last published in full at 77 Fed Reg. 21809, which is exempt from certain individual notice provisions of the Privacy Act because notifying the subject before collecting information could compromise the existence of an actual or potential confidential investigation. See [28 C.F.R. § 16.98](#).

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.*

Data collected is dictated by the search warrant. While additional voluntary information can be provided, this would be documented through a consent form (usually written) prior to the evidence being submitted to the Digital Evidence Laboratory. Due to the law enforcement nature of this system, individuals may not access, correct or amend their PII, and the system of records has been exempted from access and amendment provisions of the Privacy Act. See [28 C.F.R. § 16.98](#).

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.*

Data is collected for criminal investigative purposes and can be provided as part of criminal or civil discovery. Individuals can request system information via the Freedom of Information Act (FOIA) or Privacy Act (PA), but the information would likely be subject to a FOIA or PA exemption. <https://www.dea.gov/foia/foia-privacy-act> Relevant evidence may also be made available to a defendant pursuant to discovery in criminal prosecution or civil action.

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): 3/31/25, expiring 3/31/2029. 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:
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: SFL9FN maintains law enforcement sensitive data that, if improperly accessed, would have a serious adverse effect on DEA operations, organizational assets, or individuals. The provisional confidentiality impact level for this type of information is "Moderate." If a loss of confidentiality, integrity, or, availability regarding this information were to occur, the worst case scenario would be that individuals may suffer identify exposure which could in extreme circumstances lead to physical harm, death, or extortion of individuals and/or the DEA itself may suffer the loss of digital evidence (known/latent prints) which could lead to the obstruction of the investigation or compromise.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the System Security and Privacy Plan (SSPP) boundaries, or other conditions. RMF Security Control assessments are conducted as part of annual Core Control, annual rolling, reauthorization, and Change Control assessment activities. DEA conducts security impact analyses of system associated changes and updates of the SSPP and other relevant information system documentation as appropriate throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorization by the DEA Authorizing Official. Changes that may significantly affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are required to be reviewed and assessed by the Senior Component Official for Privacy, or a duly authorized official, prior to reauthorization by the Authorization

	Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement. Active monitoring utilizing DEA enterprise tools such as cloud-native cybersecurity platforms are conducted by the ISSO and DEACORE on an ad-hoc basis and as part of scheduled Continuous Monitoring activities. DEA's enterprise tool integrations report to the DOJ Security Posture Dashboard Report (SPDR). Additionally, SFL9FN has implemented an internal security program, to manage and provide endpoint security, enforce policies, and threat responses for assets which cannot be onboarded into the enterprise tools.
X	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted: Audit review and analysis are conducted regularly, generally, once a week.
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. All contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, Contractor Privacy Requirements; and DOJ Clause 05, Security of Information and Information Systems) and language required listed in each contract awarded within DEA.
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: DEA required training is distributed and tracked via the DOJ Learning Management System DEALS. This training includes general mandatory annual trainings for information systems, such as Rules of Behavior and Cyber Security awareness training that are applicable to all DEA component personnel. Additional training is provided for all standard users of the system (examiners). The SFL9-FN environment is used in part for portions of the training program, addressed on day one prior to gaining access. Examiners are trained in the use of SFL9FN. Privacy is covered as part of the training for staff using SFL9FN. In addition, DEA provides more in-depth, required role-based refresher privacy training annually.

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?

Key Physical Controls: Security controls like physical and environmental (PE) controls are utilized where applicable as per DOJ requirements. The SFL9FN system is isolated from all other networks and maintains a single limited inter-connect to DEA's network. The network is only accessible from within DEA laboratory-controlled spaces through role-based access controls and to individually authorized users through role-based controls accessing the system through the DEA network interconnect. Access to the system itself is protected by authentication controls, role-based access controls, and system auditing. Access to the building where the system is housed is protected by physical building security, including security guards, access badges, and security cameras.

Key Technical Controls for SFL9FN data in Transit and at Rest: The security assessments and authorizations for Certification and Accreditation adhere to the standard implemented in Cyber Security Assessment and Management system. Identification and authentication controls are utilized in SFL9FN. User Access to SFL9FN must electronically be verified and accepted.

Key Administrative Controls: Data stored in SFL9FN can only be accessed by authorized personnel who are employed by the laboratory and have been approved by Senior Laboratory Management. Customers of the laboratory (submitting case agents and their investigative teams) are only granted read-only access to their data. Additionally, all users must have access to DEA's Account Management System (AMS).² The AMS provides automated account management solutions for the DEA workforce by giving supervisors and managers the ability to manage DEA IT network and application accounts and accesses for their employees, contractors, task force officers, and other federal employees working for DEA, and includes an interactive portal for system administration personnel to track account management requests submitted by supervisors and managers. Access to individual electronic case files stored within SFL9FN is limited to those authorized laboratory personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file. The system was specifically designed to "silo" or isolate data by investigative case. This was done intentionally to make it impossible to search or review data across multiple cases at the same time.

Another administrative control is the AT (Awareness and Training) control. All laboratory staff are required to attend training prior to being granted access to SFL9FN. Each user must also complete the Cybersecurity Awareness Training and Records and Information Management training annually. This control helps employees to understand the importance of security measures and procedures and how to recognize and respond to potential threats. Moreover, SFL9FN users must read and sign DEA's rules of behavior. All DEA employees and federal contractors agree to and certify to the DEA Standards of Conduct on an annual basis.

Access to individual electronic case files stored within SFL9FN is limited to those authorized laboratory personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file.

The final work product of the digital forensics examiner (findings) is presented to DEA case agents through a virtual machine / remote desktop connection accessible from within DEA's internal network. The case agent(s) can only view content associated with their case and does not have the ability to download files, print files, or have direct access to the evidence. The final work products of

² AMS is covered by separate privacy compliance documentation.

the laboratory, which are contained in portable hard drives or Blu-ray discs, are mailed to the case agent via controlled carrier outside of the SFL9FN network. The case agent may disseminate SFL9FN results further to a prosecutor as necessary for a specific case. The case agent may also disseminate information to state or local law enforcement who have a need to know for a specific case or investigation. Likewise, such information would also be subject to criminal discovery in the event of a prosecution. However, any dissemination beyond the case agent is outside the SFL9FN system.

Finally, to further prevent unauthorized use by employees, audit logs are kept and checked at regular intervals. Cybersecurity Investigation & Response Unit (TCVV) routinely provides independent auditing against DEA security policies which provides ongoing risk mitigation to any discovered vulnerabilities as an independent entity outside of the project office. System auditing functions also allow administrators to track actions within the system.

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.)*

All data is purged from SFL9FN annually once the investigative case file has been closed. Per the DEA Record Information System (DEARIS), official records required to be maintained are extracted from SFL9FN to a hard disk or hard drive and placed in the investigative case file or non-drug evidence locker/storage until disposition. See DEARIS DEA File Number (DFN) 610-37 (N1-170-04-10) and DFN 610-38 (N1-170-06-2). Additionally, the Digital Evidence Laboratory reserves the right to purge data early (traditionally no longer than 24-36 months after receipt) depending on the availability of network storage. Any official records that are required to be maintained will be placed into the investigative case file or non-drug evidence locker/storage prior to data being purged from SFL9FN.

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.

NOTE: Data in individual silos is organized based upon the case number of the investigation from where the evidence came. Information within the silos can be retrieved via forensic tools that include searching for personal identifiers. After analysis, SFL9FN findings are downloaded to hard disk and stored in the official system of record, the relevant investigative files, and thereafter can be searched via personal identifier.

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

To the extent that information is held within SFL9FN before and after transfer to the hard disk

official record in the relevant investigative files, the data is covered by JUSTICE/DEA-008, *Investigative Reporting and Filing System*, last published in full at [77 Fed. Reg. 21809](#).

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.*

a. Potential Threats Related to the Collection of Information

Privacy Risk: Individuals that are not subject of a search warrant or consent agreement may be unaware their PII is being collected and cannot meaningfully consent to the collection of their PII.

Mitigation. This risk is partly mitigated. No individualized notice is provided by the digital evidence lab. Unless a case agent notifies individuals during the collection process or they are notified through other systems/applications prior to the evidence being entered into the SFL9FN system. Individuals who are not the subject of the legal process may not be notified the DEA is collecting their data. Because this system is used for a law enforcement purpose and contains sensitive information related to criminal and civil investigations, it is not feasible or advisable to provide notice to individuals at the time their information is accessed by the system. DEA keeps track of the details of SFL9FN entries for subsequent notification in discovery in criminal or civil cases. No notification beforehand can be accommodated due to the risk of compromising ongoing investigations.

Privacy Risk: Some PII collected may not be directly relevant and necessary for the system to accomplish its mission, including from individuals unrelated to the investigation.

Mitigation: This risk is partially mitigated. This is an evidence system and collected evidence of the electronic device or digital media, even that which is ultimately deemed irrelevant to the investigation, needs to and will be preserved for chain of custody purposes, but will be preserved as a hard disk or hard drive in non-drug evidence storage rooms or in the case file until disposition. The laboratory will maintain a copy of all work product and supporting documentation on a hard drive that is placed into a hardcopy laboratory case file prior to data being purged from SFL9FN. See DEARIS DEA File Number (DFN) 610-37 (N1-170-04-10) and DFN 610-38 (N1-170-06-2). Additionally, the Digital Evidence Laboratory reserves the right to purge laboratory data early (traditionally 24-36 months after

receipt for remaining data) depending on the availability of network storage.

b. Potential Threats Related to the Dissemination of Information

Privacy Risk: DEA personnel may share or disclose PII to an inappropriate party or for a purpose incompatible with the original collection.

Mitigation: This risk is mitigated in part. Material in SFL9FN will only be disclosed when required in criminal or civil discovery in coordination with the DEA Office of Chief Counsel. If SFL9FN material is requested via FOIA or PA request, any disclosure or withholding determination as required by law will be made in coordination with the DEA Office of Chief Counsel. The risk of unintentional disclosure is further mitigated as DEA case agents do not have the ability to review, but cannot transfer or download material from the system.

As noted above, SFL9FN material is disseminated to the case agent as part of the criminal investigation that then becomes part of the investigative file system of records. Evidence is usually preserved in an evidence file format. This format is not readable without forensic tools. It is made and returned for preservation purposes. It is sealed in a heat-sealed evidence envelope, checked back into evidence, and retained at the division until case closure. SFL9FN disseminates an examiner report with the evidence which is readable and is what the agents interact with. The case agent may disseminate information from the report further to the prosecutor as necessary for a specific case. The case agent may also disseminate information to state or local law enforcement who have a need to know for a specific case or investigation. This information sharing is done pursuant to DEA information-sharing policies and applicable routine uses for law enforcement investigation materials. However, there is no direct access by the prosecutor or the state or local law enforcement to SFL9FN.