Drug Enforcement Administration

Privacy Impact Assessment
for the
EPIC Inquiry System (EIS)
(Formerly, EPIC Seizure System)

Issued by:

James Robert Bryden
Senior Agency Official for Privacy
Drug Enforcement Administration

Approved by: Andrew McFarland
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: July 21, 2025

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

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

The El Paso Intelligence Center (EPIC) Inquiry System (EIS), formerly the EPIC Seizure System (ESS), is a Drug Enforcement Administration (DEA) system developed to enhance the capability of the DEA and other law enforcement entities in investigating, disrupting, and deterring criminal activities. This system provides authorized law enforcement personnel with access to a range of information maintained by or available to the DEA, facilitated through the EPIC System Portal (ESP) a secure internet connection, or by contacting EPIC via phone or email. EIS operates as an entry point for vetted law enforcement users, enabling them to submit requests for information from various data sources and receive results in near real-time. This Privacy Impact Assessment (PIA) is being conducted to address the changes and enhancements made to the EIS since the last PIA was drafted in 2006. These updates include the integration of new subsystems, expanded access to external datasets, and the forthcoming transition of EIS into the broader DEA Firebird network, which will re-enforce security and operational efficiency.

EIS provides law enforcement personnel access to sensitive but unclassified criminal law enforcement information obtained from federal, state, local, tribal, and international law enforcement agencies performing legitimate law enforcement interdiction and investigative duties. Federal, State and local law enforcement personnel may use the system to make inquiries related to illegal and diverted drugs; money laundering; firearms trafficking, and alien smuggling that is associated with drug related activities. Additionally, the system may be used to inquire about any other criminal activities that fall within the statutory authority of the requesting law enforcement personnel.

Data in EIS includes information about individuals, vessels, aircraft, unmanned aerial vehicles (drones), vehicles and criminal organizations, including but not limited to seizures-related activities. This information includes photographs of suspect vehicles, contraband, subjects or suspects, and identifying information about criminal offenders (e.g., name, address, date of birth, birthplace, physical description). The system also contains audit logs that capture information about the requestor and the query being made.

EIS incorporates subsystems and applications that aid in analyzing trends and identifying patterns of criminal activities. EIS's framework for accessing, using, and sharing information adheres to federal guidelines, including the National Institute of Standards and Technology (NIST) Special Publication 800-53, which outlines security and privacy controls for federal information systems, and DOJ Order 601. A permission-based access system is in place, where agency data is shared on a need-to-know basis. This ensures the relevancy of the data shared and maintains privacy controls.

DEA controls access to EIS through a vetting process, including background screening and verification of professional credentials. Non-DEA law enforcement personnel seeking access to EIS must provide personally identifying information and information about their employing agency. The applicant's Supervisor, along with the respective agency's security coordinator (if applicable) must

confirm with EPIC's User Access Management (UAM) team that the applicant is authorized to access the system and must confirm that the individual requesting access has an official need for accessing the EIS system to perform their duties. The EPIC UAM team assigns access levels based on the role and necessity of the individual, ensuring adherence to the principle of least privilege.

The security measures within EIS comprise a multi-layered encryption and continuous network monitoring regime. Regular security audits are conducted to ensure the system's defenses remain robust against known and emerging threats. EIS integrates an auditing system that logs all user activities, including information about the users and the queries being made. These logs are subject to regular audits to ensure proper usage and compliance with established guidelines. The system's secure internet connection is fortified with advanced encryption and intrusion detection systems, ensuring the integrity and confidentiality of sensitive data. EIS adheres to a structured data management protocol where information is regularly updated and outdated or inaccurate information is removed.

This Privacy Impact Assessment is being conducted as DEA is developing a new security architecture for EIS's subsystems and applications. This development will transition EIS from a standalone system to one that is integrated into DEA's Firebird internal network.[1] This integration will enhance the system's security and operational efficiency, ensuring better alignment with current technological standards and DEA's overarching IT strategy.

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 EPIC Inquiry System (EIS), formerly the EPIC Seizure System (ESS), is a system used by DEA in its efforts to combat drug-related crimes and to enhance the capability of other law enforcement entities to conduct their investigations. The principal purpose of EIS is to provide authorized law enforcement personnel access to the range of detailed law enforcement data and information maintained by or available to the DEA to assist in developing leads, identifying potential offenders, preparing documents and evidence, and ultimately assisting in prosecuting drug-related cases and associated offenses within each agency's statutory authority to enforce.

EIS was developed in 2004 and released in 2006 as a standalone system to integrate DEA's legacy Clandestine Laboratory Seizure System, a database that provided information on seizures of criminal laboratories using dangerous chemicals to manufacture narcotics, and the Automated Intelligence Records System (Pathfinder), a database that collected computerized and manual intelligence information from DEA and the former Immigration and Naturalization Service (now Customs and Border Protection) to produce association and link analysis reports and investigative records that could then be queried by Federal, state, and local law enforcement. Its purpose was to merge these

[1] Firebird will be covered under separate privacy documentation.

previously existing systems into a single, comprehensive record collection now contained in the EPIC Internal Database (discussed below). This integration provided a national shared comprehensive intelligence database for drug seizure information and related drug movement activities. It also enabled the timely analysis and dissemination of this information to the law enforcement community across the nation. Access to additional sources of information from within and outside DEA have been added over time. Information on EIS is made available to authorized users within DEA and at other Federal, State and local law enforcement agencies by means of a secure internet connection, the EPIC System Portal (ESP) (https://esp.usdoj.gov), or by contacting EPIC via phone or email for a facilitated search to more effectively investigate, disrupt and deter drug-related and other criminal activities.

Access to ESP is determined through a vetting process, which requires background screening, verification of professional credentials, and supervisor approval. Authorized users are provisioned Level-1 access given to federal, state, and local agencies personnel. ESP provides authorized users with access to a wide range of datasets, including DEA-maintained datasets, federal law enforcement repositories, and hybrid federal-state-local datasets that support criminal investigations and interdiction efforts. Access to non-DEA datasets is controlled based on DEA's internal authorization policies and Memoranda of Understanding (MOUs) with partner agencies that define the scope of permissible data queries and sharing policies, and are only directly accessible to EIS privileged users. These agreements allow DEA to retrieve and provide relevant data to vetted users without requiring the user to hold direct credentials for each external system.

Each dataset serves a specific investigative purpose, ranging from intelligence on drug interdictions and criminal organizations to real-time law enforcement alerts and historical case records. The following sections provide a detailed breakdown of the datasets available through EIS, their sources, and the specific types of information they contain.

DEA DATASETS

EIS collects, maintains, and shares information from the following DEA sub-applications located on the EIS system:[2]

- **Law Enforcement Inquiry and Alerts (LEIA).** LEIA is a core component of the EIS as it provides a federated search capability that enables authorized users to submit queries against multiple law enforcement databases. LEIA functions as a centralized request and response system, facilitating the collection, analysis, and dissemination of law enforcement information. LEIA allows federated searches across DEA owned datasets as well as external repositories. When a query is submitted, LEIA retrieves and compiles relevant results from connected

[2] The two main sources of data in the DEA datasets are: Information provided by EPIC users when requesting data, along with the results of queries conducted by EPIC personnel (Watch personnel) to respond to these requests. Both inquiry requests and query results are documented in the system. Watch personnel uploads the data to the system, except for data that is already available in the system; and Seizures reported by Federal Law Enforcement Agencies.

To ensure data quality in the process, the Watch has a supervisor who reviews inquiries and responses provided to EPIC users. For seizure data, a dedicated team reviews data entry made by Federal Law Enforcement Agencies on a daily basis. See also SORN Justice/DEA-022, El Paso Intelligence Center (EPIC) Seizure System.

systems. However, certain external databases are not directly interconnected with LEIA, requiring EPIC personal to conduct manual queries and input results into LEIA on behalf of the requesting authorized user. The system also serves as a documentation tool, recording all user-submitted requests and generated responses for accountability and auditability purposes**.**

- **National Seizure System (NSS).** National repository for collecting information on interdiction, investigation, and/or clandestine laboratory seizures; contraband (chemicals/precursors, currency, drugs, equipment, and weapons); seizure locations; persons linked to seizures, organizations; and transportation (aircraft, vehicles, and vessels). Much of this information is entered by DEA Special Agents from their investigative reports (DEA-6) or by other federal law enforcement personnel from their investigations or operations, and this information is covered by the DEA IMPACT PIA.

- **Fountainhead.** Fountainhead is an information sharing database for law enforcement to exchange marking information, impressions, and logos associated with seized packages of drugs. Fountainhead contains information including images, details of marking logos, seizure locations, quantities and associated trafficking intelligence submitted by DEA and other Federal, State, and local, and foreign law enforcement agencies. Note: the DEA IMPACT PIA covers information in Fountainhead.

- **EPIC Internal Database (EID).** The EID is an archived repository for seizure information relating to drugs and weapons trafficking; and drug-related currency seizures reported to EPIC by federal, state, and local law enforcement agencies from 1970 through 1999. EID includes personal identifiers, such as names, addresses, and telephone numbers of individuals investigated, arrested, or associated with drug trafficking activities, as well as those whose property has been seized. It also contains incident information, businesses and organizations identifiers, seizure information and identifying information on vehicles, aircraft, and vessels.

- **EPIC Law Enforcement Information Search and Analysis (ELISA).** ELISA is an archived repository of requests for inquiries submitted to EPIC by authorized EPIC users. ELISA contains inquiries concerning individuals, organizations, vehicles, vessels, and aircraft to include summary results and point of contact information. ELISA was the predecessor of LEIA.

- **EPIC-10.** The EPIC-10 is an archived repository of requests for inquires submitted to EPIC by authorized EPIC users. The EPIC-10 contains inquiries concerning individuals, organizations, vehicles, vessels, and aircraft to include summary results and point of contact information. EPIC-10 was the predecessor of ELISA.

- **Drug Precursor Database (DPD).** The DPD is an archived repository developed to track violations of pseudoephedrine sales laws, particularly to combat a tactic known as “smurfing” where individuals made multiple small purchases of pseudoephedrine to evade legal limits and supply methamphetamine production. The DPD consolidated state and local law enforcement reports of violators, containing customer's names, driver license information, address, phone information, store name, store address, store number, and store telephone number where the

Pseudoephedrine was purchased. The DPD has been an archived repository since 2010, though its historical records remain accessible for law enforcement queries through the EIS.

- **Narcotics and Dangerous Drugs Information System (NADDIS).** NADDIS is a database maintained by the DEA and contains information about individuals, organizations, businesses, and other entities that are suspected of being involved in the illicit manufacture, distribution, sale or possession of, or trafficking of controlled substances or related activities. NADDIS is a centralized automated index at DEA organized by subjects (names and/or numbers) cited in and extracted from DEA-6 investigative report forms extracted from the DEA's Investigative Management Program and Case Tracking System (IMPACT). The DEA-6 investigative report contains case related investigative information including suspect and subject identification, investigative actions taken, findings, leads, drug seizures details and connections to criminal organizations. NADDIS has two indices representing a name index and a number index which are used to access one or more specific records for examination. The system serves as both an index to the more voluminous written reports upon which it is based and as an autonomous means for developing investigative leads and aids in selecting source materials for studies of a strategic nature.

  However, EIS only has the ability to conduct searches of this dataset but does not hold or replicate all NADDIS data on EIS' servers. EIS maintains only positive inquiry results from NADDIS in EIS proper. Further, NADDIS is not directly accessible by non-DEA EIS users. Only where a non-DEA user makes a request through EPIC would a NADDIS search be run, and pointer information provided to non-DEA users. *Note: the DEA IMPACT PIA covers information in NADDIS.* https://www.dea.gov/foia/privacy-impact-assessment

OTHER FEDERAL DATASETS

A key aspect of the EIS is that it is that it serves as a portal for searching, collecting, maintaining, and sharing data obtained from other Federal law enforcement agencies' databases. EIS only retains information from searches that result in information returned and does not replicate entire datasets from these Federal systems. Although general users from other Federal agencies or State and local Law Enforcement can perform queries of EIS via direct login through the ESP, they can only access general information[3] from databases located on the EIS. To access Federal systems, users must contact the EPIC General Watch where EPIC personnel can perform queries on their behalf. Results of returns via EPIC Watch are manual uploaded by Watch personnel, and only if deemed relevant to the request. Federal information systems currently sharing law enforcement data through EIS include:

- **National Crime Information Center (NCIC).** NCIC is a computerized database of criminal justice information available to law enforcement agencies nationwide that can be separately queried by EPIC personnel. Search results must be manually added into the LEIA system. It is operated by the Federal Bureau of Investigation (FBI) and is used to assist law enforcement in apprehending fugitives, locating missing persons, recovering stolen property, and identifying terrorists. Information in the NCIC includes data on wanted persons, missing persons,

[3] Investigative information and the point of contact for any potential investigations are kept separately and will not be returned via the ESP.

unidentified persons, stolen property, and more. This system helps law enforcement agencies across the United States to share and access information about crimes and suspects. *See FBI PIA for NCIC,* https://www.fbi.gov/file-repository/pia-ncic-020723.pdf/view *and the DOJ Web Interface for NCIC PIA at* https://www.justice.gov/d9/2023-11/pia-jmd-justice_web_interface_to_ncic_jwin-final-_for_publication_0.pdf

- **TECS System, CBP Primary and Secondary Processing (TECS).** TECS (no longer an acronym) is owned by the U.S. Department of Homeland Security's (DHS), U.S. Customs and Border Protection (CBP). TECS, formerly known as the Treasure Enforcement Communication System, is an automated enforcement and inspection system designed to assist CBP Officers with screening and determinations regarding admissibility of arriving persons that can be separately queried by EPIC personnel. Search results must be manually added into the LEIA system. TECS also serves as a data repository to support law enforcement "lookouts," border screening, and reporting for CBP's primary and secondary inspection processes. *See DHS TECS PIAs at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-sar-update_0.pdf *and* https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-tecs-december2010_0.pdf

- **The Central Index System II (CIS2).** CIS2 is a database maintained by the DHS, U.S. Citizenship and Immigration Services (USCIS) that can be separately queried by EPIC personnel. Search results must be manually added into the LEIA system. This system stores records of individuals who have applied for immigration and non-immigration benefits, lawful permanent residents, naturalized citizens, United States border crossers, aliens who illegally entered the United States, aliens who have been issued employment authorization documents, individuals who petitioned for benefits on behalf of family members, and other individuals subject to the provisions of the Immigration and Nationality Act (INA). It serves as a resource for tracking the status and history of these applications. *See DHS CIS2 PIA at* https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-cis2-december2018.pdf

- **Aircraft Registration System and Airmen Registration System (ARS).** ARS is a system owned by the Federal Aviation Administration (FAA). The Aircraft Registration System is used for the registration of all aircraft in the United States. In this system, each aircraft is cataloged with specific details such as make, model, serial number, and owner information, and is assigned a unique "N-number" for identification. Similarly, the Airmen Registration System is focused on the individuals operating these aircraft. It maintains records of pilots, flight instructors, and other airmen, including their certification statuses, qualifications, and medical certifications. Level-1 users can query ARS via direct login through the ESP. However, the system will only indicate the existence and quantity of records. To obtain detailed information, Level-1 users must contact the General Watch, where EPIC personnel can perform queries on their behalf. See FAA ARS PIA at https://www.transportation.gov/individuals/privacy/pia-airmenaircraft-registry-modernization-system

- **SENTRY.** The SENTRY system, operated by the United States Federal Bureau of Prisons (BOP), is a database designed to manage and monitor various aspects of the federal prison system that can be separately queried by EPIC personnel. Search results must be manually

added into the LEIA system. This system tracks information about federal inmates, including their personal data, criminal history, and specifics of their current incarceration, including custody classification, and sentencing information. *See BOP SENTRY PIA at* https://www.bop.gov/foia/docs/sentry.pdf

- **Justice Detainee Information System (JDIS).** Is an automated system owned by the United States Marshals Service (USMS) that can be separately queried by EPIC personnel. Search results must be manually added into the LEIA system. It is used to manage records and information collected during USMS' investigations of fugitives, inappropriate communications, and threats. The JDIS is also the repository for all Federal Warrants and contains fugitive and warrant information including photographs, aliases, dates of birth, Social Security numbers, mannerisms, fingerprint codes, hangouts, vehicles, employers, numerical identifier used by other law enforcement agencies, home and business addresses, and phone numbers in addition to other known information's not listed. *See USMS JDIS PIA at* https://www.justice.gov/opcl/docs/jdis-pia.pdf

- **National Data Exchange (N-DEX).** The FBI brings together data from law enforcement agencies throughout the U.S., including incident and case reports, booking and incarceration data, and parole/probation information. It also detects relationships between people, vehicles/property, location, and/or crime characteristics. Level-1 users can query N-DEX via direct login through the ESP. However, the system will only indicate the existence and quantity of records. To obtain detailed information, Level-1 users must contact the General Watch, where EPIC personnel can perform queries on their behalf. *See FBI N-DEX PIA at* https://www.fbi.gov/file-repository/pia-national-data-exchange-n-dex-system.pdf/view

- **Federal Motor Carrier Safety Administration (FMCSA) Portal.** Is a system of the Department of Transportation (DOT) that can be separately queried by EPIC personnel. Search results must be manually added in the LEIA system. The FMCSA Portal serves as DOT's centralized database offering data critical for ensuring the safety and compliance of motor carriers and hazardous material shippers. It integrates various systems such as the Motor Carrier Management Information System (MCMIS), which provides detailed records on carriers' safety performance, and the Safety Measurement System (SMS), which quantifies on-road safety performance to prioritize intervention efforts. The SAFER System is another integral part of the database, offering access to Carrier Snapshots that detail a carrier's identification, size, commodity information, and safety records. *See DOT FMCSA PIA at* https://www.transportation.gov/individuals/privacy/privacy-impact-assessments/fmcsa-portal

HYBRID FEDERAL-STATE-LOCAL DATASETS

The EIS also collects information pursuant to authorized law enforcement activities by state and local law enforcement and integrates federal data to serve as a more comprehensive tool for authorized users to investigate, disrupt, and deter a spectrum of criminal activities. ESP users can query these hybrid datasets, via direct login through the ESP. However, the system will only indicate the existence and quantity of records. To obtain detailed information, general users must contact the General Watch, where EPIC personnel can perform queries on their behalf. EIS has a pointer system for these datasets.

Watch personnel access NLETS and NDEX through the LEIA and LEIA will automatically create a record of responsive information. The two main hybrid datasets are:

- **National Law Enforcement Telecommunications Systems (NLETS).** NLETS is a private not for profit corporation owned by all the States that enables state, local, and federal law enforcement agencies across the United States to access and exchange critical information. This system facilitates the sharing of data such as criminal history records, motor vehicle and driver's data, firearms registrations, and more, enhancing the ability of law enforcement agencies to perform background checks, track stolen property, locate missing persons, and manage other vital law enforcement activities. NLETS plays a key role in supporting the law enforcement community by providing a secure and efficient means of communication and data exchange.

- **DEA National License Plate Reader Program (NLPRP)** – The NLPRP is a law enforcement tool developed and used by DEA to enforce Title 21 authorities by facilitating the investigation of drug trafficking, bulk cash smuggling and other illegal activities associated with the drug trade. The NLPRP Network is a network of license plate reader (LPR) camera equipment owned by DEA on high-level drug and money trafficking corridors, as well as other LPR cameras owned by federal agencies, and partner state, local, tribal, and other entities with special law enforcement jurisdiction, on public roadways nationwide. NLPRP data is held on a separate system from EIS. Direct access to NLPRP requires a DEA Special Intelligence Link account though queries may be made by EPIC personnel through EIS on behalf of Level-1 users. *See DEA NLPRP-DEASIL PIA at https://www.dea.gov/sites/default/files/2025-01/DEA%20NLPRP%20DEASIL%20PIA%20Revision%20-%20Final%2020241220.pdf*

By providing a unified access point, or point of entry, the EIS streamlines the process for vetted law enforcement users to request and obtain relevant information from an extensive range of data sources available to EPIC. *See, Authorized Users section, below.* Results obtained through a search of EIS databases are provided in near real time to the user. This capability ensures that law enforcement officers can access vital information swiftly, enhancing their ability to respond to evolving situations on the ground.

SPECIFIC INFORMATION AVAILABLE

In its role as a central information hub, EIS caters to a broad array of law enforcement needs and provides access to detailed data for identifying individuals with prior criminal offenses, those undergoing the criminal justice process; and aids in comprehensive counterdrug or criminal investigations. As noted, the EIS collects investigative and intelligence reports from federal, state, local, tribal, and international law enforcement, and regulatory agencies. This integration of diverse data sources enhances the system's utility in providing a holistic view of the criminal landscape, facilitating more effective and informed law enforcement actions. These collaborations have enabled DEA to build a robust information system. The specific types of information housed in the EIS include the following:

- Seizure information on individuals, vehicles, vessels, aircraft, unmanned aerial vehicles (drones), contraband manufacturing laboratories, and criminal organizations, including photographs of suspect vehicles, contraband, and individuals who are subjects or suspects;
- Identifying information about individuals who are subjects, suspects, and criminal offenders (e.g., name, address, date of birth, birthplace, physical description, driver's license information, criminal history);
- Reports of arrests;
- Wanted persons information;
- Warrants issued for various offenses;
- Naturalization information, Alien registration, deportations, country of birth;
- Information on individuals crossing into the United States
- Information related to organizations involved in the illicit trade in controlled substances either in the United States or internationally;
- Information involving the illicit possession, manufacture, sale, purchase, and transport of controlled substances;
- Information involving the illicit manufacture, distribution, sale or possession, trafficking in or alteration of identification documents, forged merchant mariner licenses and/or merchant mariner documents (including any potentially identifiable information contained therein);
- Information relating to terrorist incidents;
- Vehicle, Vessel, and aircraft data (including registered owners);
- Commercial motor carriers' data;
- Information on stolen aircraft;
- Information on drone incidents (including registered owners);
- Counterdrug enforcement information; and
- Multi-source drug intelligence data;

INFORMATION SHARING AVENUES

EIS information is not only essential for the DEA but also for other law enforcement agencies, aiding significantly in fulfilling their diverse law enforcement responsibilities. Information in the EIS is disseminated to personnel from Federal, State, local, and tribal law enforcement agencies through the EPIC System Portal (ESP) or by contacting EPIC personnel by phone or email. The ESP serves as an online portal providing authorized users with access to the EIS. Although queries of EIS can be performed by Level-1 users (from other Federal agencies or State and local Law Enforcement) via direct login via the ESP, these users can only obtain general information from databases located on the EIS. For more in-depth queries, users must contact the EPIC General Watch (hereinafter EPIC Watch). Users who wish to export information from EIS may download the LEIA record as a PDF.

Generally, Level-1 users contact EPIC through EPIC Watch; a DEA call center staffed 24-hours a day, 7-days a week that provides immediate, real-time support to Federal, state, local, and tribal law enforcement officers. The EPIC Watch assists law enforcement with all threats and all crimes, not strictly drug trafficking investigations. The EPIC Watch provides query responses, via encrypted email of PDF files of the LEIA return, from multiple federal databases to enhance officer safety and awareness, provide instant case coordination, and assist case development. Requests from Level-1 users requiring additional levels of support are transferred to other sections at EPIC.

There is also potential for future partnerships with other Federal, State and local law enforcement agencies to share their information with EIS. EIS provides an operational framework to enhance case coordination. When information is queried and retrieved from the above-mentioned systems and repositories, EIS retains the results within the system, making it readily available for new queries on the same subject. EIS maintains audit tables that record the specific parameters of each query, the identity of the requester, and the precise date and time of the query. This approach helps identify overlaps between different cases, streamlining the investigative process and preventing duplication of efforts.

AUTHORIZED USERS

Individuals who may access or request information through the ESP include Law Enforcement Officers, as well as support staff such as intelligence analysts, dispatchers, and government attorneys involved in criminal investigations. To gain access, DEA users are required to complete a background investigation and demonstrate a legitimate professional need to use the EIS. Those not affiliated with DEA seeking access to ESP must first undergo a vetting process by EPIC. Prospective users are required to undergo background screening, providing personal identification details and information pertaining to their employing agency. Approval for access must come from the applicant's Supervisor and their agency's security coordinator (if applicable), who must verify that the individual has a valid need to access the EIS for their official duties. Access to ESP applications is provisioned through role-based access control assignments within the DOJ's Identity, Credential, and Access Management (ICAM) environment. These accounts, commonly referred to as ESP Level-1 accounts, are separate from internal EIS systems and are available to both internal and external users who meet the required access criteria. It is important to note that the "Level-1" designation applies only within certain EIS applications and does not reflect a global or system-wide access level.

Within the LEIA application specifically, user access is governed by a three-tier internal access structure that adheres to the principle of least privilege. Non-DEA users , who are general state, local, and federal customers, are provisioned as general users, referred to as "Level-1" users and can only access EPIC owned databases (EID, EPIC 10, ELISA, LEIA, NSS and DPD) through LEIA. These users must opt-in to search each database, and the scope of searchable information is limited. Level-1 users can search NDEX, NLETS and NLPRP, through LEIA but they are only notified if any records are found. Level-2 users include Watch personnel and EPIC support staff, such as intelligence analysts. This level of access is restricted to EPIC employees only. Level-2 users have full access to all EPIC-owned databases and have access to all interconnected external databases within EIS, as well as those requiring separate access. Level-3 users are limited to supervisory personnel, such as the Watch Commander and members of the EPIC supervisory chain. In addition to Level-2 access, Level-

3 users have the ability to perform workflow approval functions. Level-2 and 3 access are restricted to use only from within the EPIC facility.

EPIC's UAM Team provides the user access management staff with account management capability for vetting and maintaining users who access the EPIC Systems Portal and the EPIC General Watch. The UAM Team maintains access authorization, user account management, user authentication, password management, privilege management, access rights allocation, access rights and privileges.

SECURITY MEASURES IN PLACE

The security measures within EIS comprises of a multi-layered encryption and continuous network monitoring. Regular security audits are conducted to ensure the system's defenses remain robust against known and emerging threats. EIS integrates an auditing system that logs all user activities, including information about the users and the queries being made. These logs are subject to regular audits to ensure proper usage and compliance with established guidelines. The system's secure internet connection is fortified with advanced encryption and intrusion detection systems, ensuring the integrity and confidentiality of sensitive data. EIS adheres to a structured data management protocol where information is regularly updated and outdated or inaccurate information is removed. These reviews are conducted daily on the NSS database by dedicated EPIC personnel to ensure accuracy because authorized state, local and federal users can manually enter data when reporting seizures.

Additionally, the ESP leverages a secure internet connection to EIS data repositories, queries, reports, and analytical support providing authorized users a single comprehensive view into EPIC's capabilities and tactical information. This access is facilitated through a multi-tiered network architecture that separates user interface components from data management systems listed in the DEA Datasets, Other Federal Datasets, and Hybrid Federal-State-local Datasets Sections indicated above. This architecture effectively compartmentalizes different network segments, reducing the risk of unauthorized data access or breaches. This separation is a key security feature, as it adds a layer of insulation minimizing direct exposure to external vulnerabilities. The ESP ensures that a user is authenticated prior to allowing entrance to any part of the system. The system will confirm that the user can access the requested features or resources needed based on the user's role.

FUTURE DEVELOPMENTS

The DEA is developing a new security architecture for the EIS' subsystems and applications. This initiative marks a transition for EIS, moving from a stand-alone system to one that is seamlessly integrated within the broader DEA internal network infrastructure called Firebird. By integrating EIS into the Firebird network, the new security architecture will enhance the system's defenses against cyber threats. This integration means that EIS will benefit from the same advanced security measures and protocols that protect the DEA network. This includes sophisticated encryption, intrusion detection systems, and regular security audits, ensuring that sensitive financial data remains secure against unauthorized access and cyber-attacks. The integration also promises to streamline operations, reducing redundancy and enhancing data flow between EIS and other systems within the DEA network. This will facilitate more efficient data sharing and process automation, leading to faster response times and reduced operational costs. Moreover, system maintenance and updates can be

more effectively managed, ensuring that EIS remains in sync with the latest technology and Federal security standards.

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	Comprehensive Drug Abuse Prevention and Control Act of 1970 (84 Stat. 1236), Reorganization Plan No. 2 of 1973 (87 Stat. 1091), and Omnibus Crime Control and Safe Streets Act of 1968 (82 Stat. 197).
	Executive Order		
	Federal Regulation		
	Agreement, memorandum of understanding, or other documented arrangement	X	Memorandum of Understanding for sharing information with Federal, state, local, tribal law enforcement agencies.
	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
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*

(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
Name	X	A, B, C and D	Names, first, middle, last and suffix of DOJ and other federal government personnel, USPERS and/or non-USPERS may be collected/disseminated.
Date of birth or age	X	A, B, C, and D	Date of birth of DOJ and other federal government personnel, USPERS, and/or non-USPERS may be collected/disseminated.
Place of birth	X	C and D	Place of birth of USPERS, and/or non-USPERS may be collected.
Sex	X	A, B, C, and D	Sex of DOJ and other federal government personnel, USPERS, and/or non-USPERS may be collected/disseminated.
Race, ethnicity or citizenship	X	A, B, C, and D	Citizenship of DOJ and other federal government personnel, USPERS, and/or non-USPERS may be collected/disseminated.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	Full SSN of DOJ and other federal government personnel, USPERS, and/or non-USPERS who hold dual citizenship may be collected/disseminated.
Tax Identification Number (TIN)	X	C and D	Tax Identification Numbers of USPERS and/or non-USPERS may be collected.
Driver's license	X	C and D	Driver's License numbers of USPERS and/or non-USPERS may be collected/disseminated.
Alien registration number	X	C and D	Alien registration number of USPERS and/or non-USPERS may be collected/disseminated.
Passport number	X	A, B, C, and D	Passport numbers of DOJ and other federal government personnel, USPERS, and non-USPERS may be collected/disseminated.
Mother's maiden name	X	C and D	Mother's maiden name of USPERS and/or non-USPERS may be collected/disseminated.

(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
Vehicle identifiers	X	A, B, C, and D	Vehicle identifiers. including drone identifiers and license plate numbers of vehicles owned by USPERS and/or non-USPERS may be collected. Such data for DOJ and other government personnel may be incidentally collected/disseminated.
Personal mailing address	X	C and D	Personal mailing address of USPERS and/or non-USPERS may be collected/disseminated.
Personal e-mail address	X	C and D	Personal email address of USPERS, and/or non-USPERS may be collected/disseminated.
Personal phone number	X	C and D	Personal phone numbers of USPERS and non-USPERS may be collected/disseminated.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information	X	A and B	Employment information on DOJ and other federal govt. personnel, and potentially State, Local, Tribal law enforcement users may be collected for purposes of access management.
Education records			
Military status or other information	X	A, B, C, and D	Military status information DOJ and other federal government. personnel, USPERS and/or non-USPERS may be collected/disseminated.
Employment status, history, or similar information	X	A, B, C, and D	Employment status information on DOJ and other federal govt. personnel, USPERS and/or non-USPERS may be collected/disseminated. Such information could include employer, agency, law enforcement officer, start date etc.
Employment performance ratings or other performance information, e.g., performance improvement plan			

(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
Certificates	X	C and D	Baptismal and birth certificates of USPERS and non-USPERS may be collected/disseminated.
Legal documents	X	C and D	Legal documents of USPERS and non-USPERS may be collected/disseminated.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	C and D	URLs of USPERS and non-USPERS may be collected.
Foreign activities	X	C and D	Foreign activities of USPERS and non-USPERS may be collected/disseminated.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Criminal record information of USPERS and non-USPERS may be collected/disseminated.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information	X	A, B, C, and D	Agency email addresses, phone numbers, and any other business-related information, on DOJ and other federal government personnel, USPERS and/or non-USPERS may be collected/disseminated.
Location information, including continuous or intermittent location tracking capabilities	X	C and D	Locations of seizures or other events related to or including the presence of USPERS and/or non-USPERS may be collected/disseminated.
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	Photographs, etc. of USPERS and non-USPERS may be collected/disseminated.
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			

(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
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C and D	Scars, marks, tattoos of USPERS and non-USPERS may be collected/disseminated.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	Audit logs
- **User passwords/codes**	X	A and B	Hashed Password/PIV code
- **IP address**	X	A and B	Audit Logs
- **Date/time of access**	X	A and B	Date/Time of Access to System
- **Queries run**	X	A and B	Audit Logs
- **Content of files accessed/reviewed**	X	A and B	Audit Logs
- **Contents of files**	X	A and B	General files
Other (please list the type of info and describe as completely as possible):	X	A and B	Other currently unknown PII records of USPERS and non-USPERS may be collected/disseminated that are not categorized here.

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):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)* (on a case-by-case basis)	X		

Government sources:
Other (specify):

* NOTE: Foreign sources may contribute to EIS data on a case-by-case basis depending on the Multilateral Legal Assistance Treaty (MLAT) or other agreement with the foreign government.

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Other (specify):					

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	The information is shared within the DEA when the purpose is to facilitate the investigation and prosecution of illegal drug trafficking activities and to support the course of investigations where necessary to elicit information pertinent to counter drug, counterterrorism, weapons, alien, and drug money investigations.
DOJ Components	X		X	The information is shared with any internal component of the Department when the purpose is to facilitate the investigation and prosecution of illegal drug trafficking activities and to support the course of investigations where necessary to elicit information pertinent to counter drug, counterterrorism, weapons, alien, and drug money investigations.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Federal entities	X		X	The information is shared with other federal law enforcement agencies. In addition, the information may also be shared in accordance with published routine uses. For a list of the published routine uses, see the System of Records Notice for DEA-022, EPIC Seizure System, 71 FR 36362 (2006). Approximately 12,000 non-DOJ federal users have direct login access.
State, local, tribal gov't entities	X		X	The information is shared with state, local, tribal, and international law enforcement agencies. In addition, the information may also be shared in accordance with published routine uses. For a list of the published routine uses, see the System of Records Notice for DEA-022, EPIC Seizure System, 71 Fed. Reg. 36362 (2006). Approximately 36,000 state and local agency users have direct login access.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			EIS records may be shared with a court or administrative body in accordance with DOJ regulations on discovery, when it is determined that the records are relevant to the proceeding.
Private sector				
Foreign governments	X			EIS information may be shared with other foreign governments on a case-by-case basis through DEA country offices.
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.

EIS does not release information 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.

EIS does not collect information directly from individuals. The other systems from which EIS pulls information are generally law enforcement related systems. All data collected from those systems is for law enforcement purposes only and contain sensitive information related to criminal and civil investigations, therefore it is not feasible or advisable in most cases to provide notice to individuals at the time their information is collected by those systems nor when such information is accessed by the EIS. However, DEA has published a Privacy Act System of Records Notice (SORN) which provides general notice at JUSTICE/DEA-022, "El Paso Intelligence Center (EPIC) Seizure System (ESS)," 71 Fed. Reg 36362 (June 26, 2006), modified by 82 Fed. Reg. 24147 (May 25, 2017 available at https://www.govinfo.gov/content/pkg/FR-2006-06-26/pdf/E6-9977.pdf [4]

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, individuals who are the subjects of EIS data inquiries do not have the opportunity to voluntarily participate in the collection, use or dissemination of their information in the system. Information pertaining to individuals is obtained from them by law enforcement agencies and/or individual officers based on their suspected involvement with illegal drug trafficking activities, criminal case investigations, or other violations of the law. There is no general opportunity to consent to particular uses of information because the information contained in the system is existing data that was lawfully gathered and maintained based on law enforcement authority and individuals may not have an opportunity to consent to particular uses of that information. Further, any forms or webpages collecting identifying information of users for access to the system requires personally identifiable information and relevant law enforcement employment information such that a privacy notice is provided.

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.

---

[4] Please note, this SORN is being revised and will be renamed El Paso Intelligence Center (EPIC) Inquiry System (EIS).

An individual who is the subject of a record in this system may access or seek amendment to those records that are not exempt from disclosure through the procedures described in 5 U.S.C. § 552a(d) and 28 C.F.R. § 16.40 et seq. for requesting access and/or amendment to Privacy Act protected records. Individuals may also request access to records under the FOIA, and exemptions apply as relevant. For a list of exemptions, please see 16 C.F.R. § 16.98 and 72 Fed. Reg. 54825 (September 27, 2007). A determination whether a record may be accessed will be made at the time a request is received.

Individuals desiring access to information maintained in the system or to contest or amend information maintained in the system may do so electronically or in writing by sending the request in an envelope and letter clearly marked 'Privacy Access Request,' That must include a general description of the records sought and must include the requester's full name, current address, and date and place of birth. An individual who is the subject of a record in this system may seek amendment or correction of those records that are not exempt pursuant to a final rule published at 72 FR 54825). If the requestor is seeking an amendment, the request should state clearly and concisely what information is being contested, the reasons for contesting it, and the proposed amendment to the information sought. The request must be signed and either notarized or submitted under penalty of perjury and dated. A determination whether a record may be amended or corrected will be made at the time a request is received.

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):** January 8, 2025 **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:** POAM 44067 is pending OPCL approval of new PIA**.**
	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:**

	DEA monitors the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system-associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, 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 reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO (Chief Privacy and Civil Liberties Officer), 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.
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:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the DEA Enterprise Digital Identification System (DEDIS)-information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with DEA Incident Response Plan. DEA TCVV monitors DEDIS using the Splunk event correlation tool to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Jira ticketing system.
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**. Yes, as a standard operating procedure, all DEA contracts provide that contractors are bound by the Privacy Act, other applicable laws and DEA and 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:** Required training is distributed and tracked via the DOJ Learning Management System – DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and Cyber Security awareness training that are applicable to all DEA component personnel. However, the Office of Chief Counsel (CC) is working on a role-based annual privacy training which will be published soon.

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?

The security measures within EIS is comprised of multi-layered encryption and continuous network monitoring. Regular security audits are conducted to ensure the system's defenses remain robust against known and emerging threats. EIS is a DEA accredited system, which is compliant with NIST 800-53 (rev 5) Security and Privacy Controls for Information Systems and Organizations. EIS follows DOJ and DEA continuous monitoring requirements in order to maintain its Authority to Operate (ATO). Compliance requirements are tracked via Plan of Action and Milestone (POAMs) within DOJ's Joint Cybersecurity Assessment and Management (JCAM) system portal, which is monitored by DEA leadership, Information Security Officers, and IT management.

The EIS repository is physically protected in compliance with Department of Justice Order guidelines for Cybersecurity Program (DOJ Order 0904) pertaining to both physical and environmental security. Hardware and electronic media used in the EIS are Federal Information Processing Standards (FIPS) 140-2 compliant and protected in accordance with the sensitivity of the data that the system is authorized to process, store, or transmit.

EIS as a whole leverages multiple defense in-depth security devices to include anti-virus protection, web content filter, intrusion prevention system, adaptive security appliance, host-based firewalls, network-based firewalls, integrated endpoint detection and response (EDR), network detection and response (NDR), log/traffic monitored by DEA and DOJ Security Operations Center (SOC).

Additionally, the ESP leverages a secure internet connection to EIS data repositories, queries, reports, and analytical support providing authorized users a single comprehensive view into EPIC's capabilities and tactical information. This access is facilitated through a multi-tiered network architecture that separates user interface components from data management systems listed in the DEA Datasets, Other Federal Datasets, and Hybrid Federal-State-local Datasets Sections indicated above. This architecture effectively compartmentalizes different network segments, reducing the risk of unauthorized data access or breaches. This separation is a key security feature, as it adds a layer of insulation minimizing direct exposure to external vulnerabilities. The ESP ensures that a user is authenticated prior to allowing entrance to any part of the system. The system will confirm that the user can access the requested features or resources needed based on the user's role.

The system's secure internet connection is fortified with advanced encryption and intrusion detection systems, ensuring the integrity and confidentiality of sensitive data. EIS adheres to a structured data management protocol where information is regularly updated and outdated or inaccurate information is removed.

EIS also integrates an auditing system that logs all user activities, including information about the users and the queries being made. These logs are subject to regular audits to ensure proper usage and compliance with established guidelines. EIS Security Personnel are responsible for viewing, monitoring, and archiving security logs and audit trails on the EIS. Audit data consist of the date, time,

subject, and originating account of all user queries. These audit logs are kept online for one year, and the previous five years are archived.

Further, all EPIC staff are required to complete the annual DEA Mandatory Cybersecurity Awareness Training (CSAT) and sign the Rules of Behavior for DEA IT systems. In addition, DEA is seeking to implement annual refresher privacy training in FY2025.

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.)

At this time, there is no approved records retention schedule for the information contained in this system. A proposed schedule has been submitted to the National Archives and Records Administration (NARA) for approval. Until NARA approval is received, all records will be treated as permanent and retained in accordance with applicable law and policy. Once the retention schedule is approved, records will be maintained and disposed of in accordance with the approved schedule. The records in source systems from which EIS may ingest information are maintained and disposed of in accordance with their appropriate DEA and NARA schedules, primarily but not exclusively those for Enforcement & Drug Control Files:

File No. 601-38 (N1-170-06-2) Evidence Files.

(A) **Nondrug Property.** Relevant DEA forms, evidence tracking system printouts, inventory records, related court orders and correspondence related to Title III material.--Disposition: Temporary. Cutoff at the close of the file annually. Destroy 2 years after close of file.

(B) **High Value Property**. Relevant DEA forms and Standard Seizure Forms, evidence tracking system information, and Consolidated Asset Tracking System printouts, abandonment correspondence(s), inventory records, and other relevant information--Disposition: Temporary. Cutoff at the close of the file annually. Destroy 6 years 3 months after close of file.

(C) **Seized Monies**. These files consist of various Relevant DEA forms, Standard Seizure Forms, evidence tracking system records, Consolidated Asset Tracking System printouts, abandonment correspondence(s), inventory records, and other relevant information--Disposition: Temporary. Cutoff at the close of the file annually. Destroy 6 years 3 months after close of file.

File No. 601-39 (DAA-0170-2013-0004) Investigative Management Program and Case Tracking (IMPACT) System files:

(A) **Output Records**: Includes central data repository and electronic storage areas for case related information and data, ad hoc inquiries and other reporting requirements. Electronically feeds to other agency internal systems, as well as electronic feeds to other law enforcement and justice entities--Disposition: Temporary. Destroy when business use ceases. (GRS 4.3, items 030/031);

(B) **Master File**: Information about DEA investigative activities (reports of investigation, arrest information, photographs, fingerprints, defendant information, financial information, asset seizure and forfeiture information, drug seizures, non-drug seizures) including:

(1) *Numbered Investigative Case Files*. DEA Reports of Investigation--Disposition: Temporary. Cut off at the close of case. Destroy/delete 25 years after case closed. (DAA-0170-2013-0004-0001) dispose of case files originated by other District or Resident Offices according to File No. 601-12; and

(2) *General Case Files*. DEA reports of investigation that are limited in scope concerning individuals, firms, ships, or related subject pertinent to violations of drug narcotic laws or DEA registrant activities--Disposition: Temporary. Cut off 6 years after last activity or last date of correspondence, whichever date is later. Destroy/delete 25 years after cut-off. (DAA-0170-2013-0004-0002)

Section 7: Privacy Act

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

_____ No. ___X__ Yes.

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

JUSTICE/DEA-022, "El Paso Intelligence Center (EPIC) Seizure System (ESS)," 71 FR 36362 (June 26, 2006), 71 Fed. Reg 36362 (June 26, 2006), modified by 82 Fed. Reg. 24147 (May 25, 2017).; 82 FR 24147 (May 25, 2017).https://www.govinfo.gov/content/pkg/FR-2006-06-26/pdf/E6-9977.pdf. Exemptions to several Privacy Act provisions have been claimed pursuant by the Attorney General See 28 C.F.R. §16.98. https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=524e56b7bd8379a830d157f937ad5a82&mc=true&n=pt28.1.16&r=PART&ty=HTML#se28.1.16_198

See also, JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May 25, 2017)(amendment). https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf

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?

a. Potential Threats Related to Information Collection

Privacy Risk: DEA and non-DEA systems providing information to EIS may be over-collecting more personally identifying information than necessary to accomplish DEA's

official duties and its mission, and EIS could be maintaining and disseminating such over-collected information.

Mitigation: This privacy risk is mitigated. DEA has implemented several measures to ensure the appropriate handling and minimization of PII. The EIS system provides authorized law enforcement users access to sensitive but unclassified criminal law enforcement information obtained in the course investigations by Federal, State, local, and tribal agencies. In general, professional law enforcement at every level, and DEA Special Agents in particular, are trained not to gather irrelevant or to gather excessive amounts personal information in their investigations. In fact, DEA has data minimization protocols to mitigate the risk of over-collection and unnecessary retention of PII. These protocols ensure that only necessary data is collected in response to requests for information from authorized users. Watch personnel who perform the facilitated queries and collect the information maintained in the EIS system follow the same approach. They extract and provide only the relevant and necessary information from DEA and non-DEA datasets to the users.

Although EIS collects data from other law enforcement systems, the system only retains information from successful query results and does not replicate entire datasets from these systems. System specific minimization protocols are in place to prevent the over-collection of PII across all datasets within EIS. For instance, the National Seizure System (NSS) collects information related to the seizure of drugs, clandestine drug manufacturing laboratories, and related contraband. PII from these seizures is limited to suspects involved in the reported seizure and is not directly provided to users requesting NSS information. Watch personnel only provide the reporting law enforcement agency's point of contact (POC) to the requestor to ensure case coordination.

Similarly, with respect to the Law Enforcement Inquiry and Alerts (LEIA) federated search dataset, investigative information is not provided to users. Rather, EPIC personnel provide the relevant investigator's POC information to ensure proper case coordination. EPIC follows the same approach for searches of the EPIC Internal Database (EID), the archived repository for seizure information related to drug and weapons trafficking and drug-related currency seizures. PII from these records is not directly provided to users by EIS and EPIC personnel only provide to the requestor the relevant investigator's POC to ensure proper case coordination. Although queries of EIS can be performed by general users (i.e., users from other Federal agencies or State and local Law Enforcement) via direct login, these users can only obtain certain, more general information from EPIC owned databases (i.e., LEIA, NSS, EID, ELISA, EPIC-10, and DPD). For more in-depth queries, users must contact the General Watch The General Watch will query all databases and share the results with the requestor.

In particular, the NADDIS dataset is held on a separate system from EIS called DEA IMPACT and not shared with non-DEA users. While DEA users have access to query NADDIS, they are trained to only query and use information relevant to their cases. When writing investigation reports, which are ultimately fed into NADDIS, DEA personnel only enter relevant facts, ensuring that the data in the system is pertinent and necessary for

ongoing investigations. See Section 2 for more information on NADDIS and DEA IMPACT.

Privacy Risk: Possibility that the PII of an unrelated individual (who is not under suspicion or the subject of investigation) is collected, maintained, and disseminated by EIS as part of an inquiry or investigation about someone else, that may not be accurate or relevant.

Mitigation: This risk is mitigated with respect to EIS use. The scope and breadth of information placed into the other information systems that EIS accesses are not within the purview of EPIC and is outside the scope of the EIS PIA. Please see the relevant PIAs for those systems. However, all information that is queried and collected into the EIS system is performed by EPIC personnel who will follow protocols to extract only relevant and necessary information from DEA and non-DEA datasets. Watch personnel are specifically trained how to query EIS datasets following requests for information from DEA and non-DEA users and how to deliver results. Mitigation includes data minimization and relevance to minimize the risk that the PII of an unrelated individual is collected. Role-based access control is also implemented to limit access to PII by denying access to certain databases, and reducing the sensitivity of the data returned from others.[5] This ensures that only authorized personnel can view or use the collected data. Regular audits and continuous monitoring of data collection, maintenance, and dissemination practices are conducted to identify and rectify instances where unrelated PII might have been captured or shared.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Potential for use of PII in a manner incompatible/inconsistent with the intended uses of or specified purposes for collection of the information or being used for an unauthorized purpose.

Mitigation. This risk is mitigated. Almost all information collected in and accessible to EIS has been collected pursuant to a law enforcement criminal investigation and any authorized users of EIS would be using EIS for similar investigations. DEA restricts access to EIS to authorized law enforcement groups, such as supervisors, law enforcement agents/officers, and task force members associated with agencies, with a need for access. To ensure only law enforcement personnel are authorized users, the system enforces robust security protocols and access controls, aligning with applicable laws, rules, and policies. Both physical and digital safeguarding measures, such as restricted building access, password protections, and audit logs, are deployed to ensure that only qualified individuals can access the sensitive information, thereby upholding the system's integrity and protecting the privacy of the individuals whose data is stored within. Additionally, a stringent verification process is in place for requestors seeking information via telephone, ensuring that data disclosure is carefully controlled.

Although there is a residual possibility that authorized users or administrators could access EIS for purposes inconsistent with the reasons for collecting the information therein, audit logs

[5] *See* Sec 2 for discussion on access restrictions for particular databases.

would exist of any questionable searches made and could be the subject of disciplinary action for improper uses. Users must also adhere to specific “Rules of Behavior" For EIS and DEA IT systems that reinforce use of DEA information system for only authorized purposes. In addition, limited access to EIS will be provided to system administration and system security groups for purposes of conducting system operation and maintenance tasks.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is partly mitigated. The disposition standards for the Federal records in this system are not currently scheduled by NARA but are pending scheduling action by NARA under DEA’s Bucket Retention Schedule. Records in this system in all formats will be maintained and disposed of in accordance with appropriate authority of the National Archives and Records Administration once approved. Although there is currently not a records retention schedule adopted for the EIS, the underlaying schedules for case information will apply to much of the information from DEA investigations in DEA datasets. Further, other underlying retention schedules will likewise apply to other record items in datasets accessible by EIS, such as the NLPRP data or third-party systems. The data from these systems are tagged when uploaded by EPIC Watch to EIS with the data source that will allow EIS administrators track and destroy the data in accordance with the relevant retention schedule.

Privacy Risk: There is a possibility that system information, either at rest or in transmission, could be susceptible to compromise without sufficient technical, and administrative privacy and security controls to protecting from technological/cyber breach (e.g., Hacking) or from an “Insider Threat” action resulting in a breach.

Mitigation: This risk is mostly mitigated. Despite the implementation of advanced security measures, some potential for unauthorized access, data breaches, and misuse of information remains. Due to the volume of records and the type of information being collected as described above, there is a risk to the privacy rights of individuals if the system becomes a target for cybercriminals and insider threats. However, to help mitigate this risk, the information in this system is safeguarded in accordance with applicable laws, rules, systems security, and access policies. Encryption of data at rest and in transit ensures that intercepted information remains confidential and unusable. Access to this system is also governed by strict policies, granting minimum necessary access based on roles and responsibilities, thereby reducing the insider threat vector.

In addition, EIS follows the governance of DOJ 0904-Cybersecurity Program and the DOJ Cyber security standards (NIST compliance) for applying security controls and safeguards to information systems. EIS employs a multi-layered defense-in-depth security approach, through a combination of perimeter and internal hardware and software security safeguard mechanisms, to ensure security controls protect organizational objectives. The security defenses include layered perimeter security safeguards and internal host-based security protection mechanisms. The perimeter architecture consists of EIS managed perimeter firewalls, perimeter routers, Next-Gen firewalls, and intrusion detection/prevention systems. Internal security protection mechanisms include endpoint protection providing host-based

malware and proactive threat protection, database encryption, Homeland Security Presidential Directive-12 Personal Identity Verification (PIV) compliance, Identity Credential and Access Management, and advanced system and event logging.

DEA also enforces secure configuration management to ensure the EIS operates in the most restrictive secure mode. EIS also follows the established DOJ and DEA continuous monitoring strategy. Continuous monitoring security protection mechanisms include using Security Information and Event Manager monitoring systems. Additionally, consistent with FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL), or other FIPS 140-2 approved encryption methods. A status of EIS MOU and ISA are maintained within the DOJ JCAM repository in accordance with the EIS System Accreditation.

Privacy Risk: DEA may not appropriately monitor, test, and evaluate privacy and security controls to safeguard PII and may inadequately perform auditing of system use to ensure compliance with security and privacy standards.

Mitigation: This risk is mitigated. DEA monitors information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, 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 reauthorizations by the DEA Authorizing Official. Significant changes that affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII will trigger an additional Initial Privacy Assessment and potentially a modification of this PIA that will be reviewed and assessed by the CPCLO (Chief Privacy and Civil Liberties Officer), or a duly authorized official. DEA ensures that the appropriate officials are made aware, in a timely manner, of any information system when it cannot be appropriately protected or secured, and that such system is given a high priority for upgrade, replacement, or retirement.

c. Potential Threats Related to Dissemination

Privacy Risk: Potential for access by DEA personnel with no authorization or no need to know the information.

Mitigation: This risk is mitigated. Only personnel who maintain the system and authorized vetted users who are members of law enforcement agencies and who have undergone background screening are permitted access to the system; and such access is limited to those who have an official need to know to perform their duties. Even though access to this system is tightly controlled through a vetting process, including background screenings, employment and authorization verification, and requiring a valid law enforcement-related reason for access, there may remain some residual risk to individuals' privacy rights.

To mitigate this risk further, several administrative and technological controls secure the information contained within EIS. The Security Administrator, the System Administrator, and the User Access Manager are three major components of the EIS administration. The Security Administrators are responsible for viewing, monitoring, and archiving security logs and audit trails. The System Administrators are responsible for the maintenance and operation of the system as a whole, including backing up the system and its recovery. The User Access Managers are responsible for adding, changing, or deleting users and their system access privileges. The determination of appropriate users and assignment of passwords are other administrative controls in place.

User Access Managers rely on individual user's supervisors to notify loss of authorization. If an account is inactive for 30 days, it is suspended; if the user does not contact EPIC within 90 days, it is deactivated. To regain access, the user must complete a reactivation process, including validation through their official work email.

DEA contractors are assigned roles based on the nature of their work. If they are IAs working for the Department, they are assigned the IA role. If they are Information Technology support personnel, they are assigned administrator, auditor, etc. roles. If their work is to provide reports, they are assigned the reports role. The system determines the user's role based upon the user profile that is stored in the database. When a user has successfully logged in, the system retains the user's role and adjusts the functionality as appropriate to that role.

Further, all EPIC staff are required to complete the annual DEA Mandatory Cybersecurity Awareness Training (CSAT). There are three categories of roles available on the system: roles related to the user's type of work (Law Enforcement Officer, Intelligence Analyst (IA), etc.); roles related specifically to applications (report role, data input role, etc.); and roles related to system functions (administrator, auditor, etc.) Each role has access permissions which control the amount and type of access to the system data. This mandated training addresses the proper and safe handling of privacy data.

Privacy Risk: Potential for EIS or authorized users of EIS to share or disclose PII Information to an inappropriate party or for an improper use or of receipt of EIS data by unauthorized recipients once data reaches its destination.

Mitigation: This risk is partially mitigated. The very purpose of the EIS system is to disseminate information to law enforcement entities at all levels of government to facilitate the investigation and prosecution of illegal drug trafficking activities and to support investigations related to counter-drug, counterterrorism, weapons, aliens, drug money investigations, and other crimes within the statutory authority of partner agencies. The information provided by EIS, including PII, is considered law enforcement sensitive. This means that the information can only be distributed to Federal Government law enforcement, public safety or protection officials, and individuals with a need to know and therefore not for public disclosure. All information and reports provided to users contain disclaimers against re-dissemination to third parties without DEA's approval. All authorized users must abide by these rules. As mentioned

above, DEA takes great care in the vetting of users in ensure they are appropriate law enforcement officers. Additionally, although queries of EIS can be performed by general users (from other Federal agencies or State and local Law Enforcement) via direct login, these users can only obtain general information from EPIC owned databases. For more in-depth queries, users must contact the General Watch. The General Watch will query all databases and share the results with the requestor. Once information from EIS has been provided to a non-DEA requestor, users must request a DEA review and approval if they need to re-disseminate the information outside the approved channels. These rules are very similar to those of other law enforcement agencies. Protecting this type of information is a common practice in the law enforcement community. In addition, DEA is also in process of providing annual role-based privacy trainings during FY2025 that will discuss the requirements for dissemination of PII beyond the Department of Justice.