Organized Crime Drug Enforcement Task Forces

Privacy Impact Assessment
for the
OCDETF Management Information System
(OCDETF MIS)

Issued by:
Kristin D. Brudy-Everett
Senior Component Official for Privacy

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

Date approved: August 15, 2025 *(March 2025 DOJ PIA Template)*

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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 OCDETF Management Information System (MIS) is a case tracking and reporting system designed to provide a platform for OCDETF investigative and prosecutorial personnel to track and coordinate investigative efforts. The purpose of this system is to support the mission of the OCDETF Program, which is to reduce the illegal drug supply by identifying, disrupting and dismantling the most significant international and domestic illegal drug supply and money laundering organizations and related criminal activities. The OCDETF MIS is used to collect data from the initiation of an OCDETF investigation through the closing of the case.

The OCDETF MIS was also designed to meet the management needs of the OCDETF Executive Committee, the Operations Chiefs Group, the Washington Agency Representatives Group (WARG), the United States Attorneys, and other participating agency officials, regions, and districts. The Executive Office for OCDETF supports the work of federal agents, prosecutors, and state and local law enforcement officers who participate in OCDETF cases. The Executive Office, in conjunction with the WARG, provides policy guidance and coordination; administrative management and support; collection and reporting of statistical information; and budgetary planning, coordination, and disbursement. To this end, the system provides the data necessary to evaluate Program performance, and to provide reports to the President, the Attorney General, the Congress, and the public.

The OCDETF MIS is an application that contains the data necessary to track cases, analyze drug trafficking trends, and evaluate program performance. All information maintained in the OCDETF MIS is contributed by OCDETF's eleven federal member agencies: DOJ's Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and the United States Marshals Service (USMS); the Department of the Treasury's Criminal Investigation Division of the Internal Revenue Service (IRS); the Department of Homeland Security's Immigration and Customs Enforcement (ICE/HSI); the United States Coast Guard (USCG); the Department of Labor (DOL); the United States Postal Inspection Service (USPIS); and the United States Secret Service (USSS); in cooperation with the DOJ's United States Attorney's Offices (USAO) and Criminal Division (CRM). These agencies collect investigative and prosecutorial information via various methods consistent with their authorities in support of their respective missions and contribute information into MIS to support OCDETF's mission work. This information is entered and uploaded into the

OCDETF MIS application by a trained USAO POC at the District or Regional level with appropriate data entry access. The OCDETF MIS provides online storage and retrieval of such investigation and prosecution information for use by OCDETF personnel. This collection of investigative information advances the coordination of law enforcement efforts in support of OCDETF's mission, facilitates data sharing among participating agencies, and provides real time information on all of OCDETF's investigative and prosecution efforts.

The OCDETF MIS application makes OCDETF case tracking and investigative and performance data available to authorized OCDETF personnel that have access to the DOJ intranet. (Authorized OCDETF personnel are described in section 2.1 below.) The OCDETF MIS application provides a paperless and simplified environment for data entry and reporting; provides OCDETF offices access to the most current data on targets, investigations and prosecutions; and contains an inventory of analytical and informational reports that enables OCDETF management and personnel to review and evaluate investigative efforts.

The Organized Crime Drug Enforcement Task Forces (OCDETF) is an independent component of the U.S. Department of Justice. Established in 1982, OCDETF is the centerpiece of the Attorney General's strategy to combat transnational organized crime and to reduce the availability of illicit narcotics in the United States through a prosecutor-led, multi-agency approach. OCDETF leverages the resources and expertise of its partners in concentrated, coordinated, long-term enterprise investigations of transnational organized crime, money laundering, and major drug trafficking networks. Today, OCDETF is the largest anti-crime task force in the country. OCDETF's overarching strategy combines priority targeting, case coordination, intelligence sharing, and directed resourcing to have the greatest impact disrupting and dismantling command and control elements of criminal organizations that impact the United States.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

Due to the nature of the data being collected, personally identifiable information regarding defendants, targets and potential targets must be collected. Many targets may have the same or similar names, or one target may use multiple names. The data includes information such as name, social security number, date of birth, FBI number, and alien registration number and citizenship for OCDETF targets/defendants. The SSN is used as

the primary, and most reliable, identifier of targets within the OCDETF MIS system. Also, narrative summaries may include other personally identifiable information. Additionally, names and DOBs of state and local officers that are paid for overtime work on OCDETF investigations are also maintained to facilitate administrative requirements. Contact information for OCDETF case agents, attorneys and other key personnel are also maintained.

Additionally, related administrative records, including information on state and local payments to state and local officers for state and local case participation is also maintained in the system. Contact information (i.e., name, phone number and email address) of case agents, case attorneys, and state and local personnel is maintained for the purpose of case tracking and coordination between agencies, and payment tracking for OCDETF state and local payments.

The OCDETF MIS advances the coordination of law enforcement efforts in support of OCDETF's mission and facilitates data sharing among participating agencies and provides real time information on all of OCDETF's investigative and prosecution efforts.

The OCDETF Program is critical to the Justice Department's intra- and inter-agency drug enforcement strategy, pursuing comprehensive, multi-agency, multi-jurisdictional investigations of major drug trafficking and money laundering organizations that are responsible for the flood of illegal drugs in the United States, and the violence generated by the drug trade. Consistent with the President's National Drug Control Strategy, which seeks to "break" the drug market by making the drug trade more costly and less profitable, OCDETF simultaneously attacks all elements of the most significant drug organizations affecting the United States. These include the international supply sources, their international and domestic transportation organizations, the regional and local distribution networks, and the violent enforcers the traffickers use to protect their lucrative business from their competitors and from the law. At the same time, OCDETF attacks the money flow that supports the drug trade – depriving drug traffickers of their criminal proceeds and the resources needed to finance future criminal activity.

OCDETF has long recognized that no single law enforcement entity is able to disrupt and dismantle sophisticated drug and money laundering organizations alone. OCDETF combines the resources and expertise of its eleven federal agency members (DEA; FBI; ATF; USMS; IRS; ICE/HSI; USCG; DOL; USPIS; USSS) in cooperation with the Department of Justice's Criminal Division, the 94 U.S. Attorneys' Offices, and state and local law enforcement, to identify, disrupt, and dismantle the drug trafficking and money laundering organizations most responsible for the Nation's supply of illegal drugs and the violence the drug trade generates and fuels. OCDETF is successful because it effectively leverages the investigative and prosecutorial strengths of each participant to combat drug-related organized crime. The OCDETF Program promotes intelligence sharing and intelligence-driven enforcement and strives to achieve maximum impact through strategic planning and coordination.

In addition, the system information facilitates management of such programs as administrative forfeitures and diversion control (preventing, detecting, and investigating the diversion of controlled pharmaceuticals and listed chemicals from legitimate sources while ensuring an adequate and uninterrupted supply for legitimate medical, commercial, and scientific needs). The OCDETF MIS also holds case report narratives, which may contain information on previously unknown methods by which organizations operate. Understanding how criminal organizations evolve enables OCDETF and its participants to better disrupt and dismantle the organizations. Further, the system provides the data necessary to evaluate Program performance and to provide reports to the President, the Attorney General, the Congress, and the public.

Information collected by the OCDETF MIS includes investigative case information from member federal law enforcement agencies and partners as well as information covered by the Bank Secrecy Act (BSA).

At a minimum, the following information is collected, maintained, used, or disseminated:

- Social Security Numbers (SSNs)
- Employer and Taxpayer Identification Numbers (EINs/TINs)
- Phone Numbers
- Dates of Birth (DoBs)
- Email Addresses
- Personal Names
- Home Addresses
- Business Addresses
- IP Addresses
- Law Enforcement Identification Numbers
- Social Media IDs/Monikers
- Passport Numbers
- Driver's License Numbers

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	- Title 5 U.S.C. § 301 - Title 21 U.S.C. § 841 - Title 21 U.S.C. § 873 - Title 21 U.S.C. § 878, Controlled Substance Act - Title 18 U.S.C.§ 2518, (1) (e), Crimes and Criminal Procedures - Consolidated Appropriations Act, 2004, Public Law 108–199, 118 Stat. 3 - Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91– 513, 84 Stat. 1236 (21 U.S.C. § 801 *et seq.*) - Organized Crime Control Act of 1970, Public Law 91–452, 84 Stat. 922
Executive Order	Executive Order 11396, 33 Fed. Reg. 2689 (1968), 3 C.F.R. 1966-1970 Comp. p. 711.
Federal regulation	*See id.*
Agreement, memorandum of understanding, or other documented arrangement	- United Nations Single Convention on Narcotic Drugs, 1961 - United Nations Convention on Transnational Organized Crime, 2000
Other (summarize and provide copy of relevant portion)	Additional authority is derived from Treaties, Statutes, Executive Orders, and Presidential Proclamations which DOJ has been charged with administering.

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)*
Name	X	A, B, C, D	
Date of birth or age	X	A, B, C, D	
Place of birth	X	A, B, C, D	
Sex	X	A, B, C, D	
Race, ethnicity, or citizenship	X	A, B, C, D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C	
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C, D	
Passport number			
Mother's maiden name			
Vehicle identifiers	X	C, D	
Personal mailing address	X	A, B, C, D	
Personal e-mail address	X	A, B, C, D	
Personal phone number	X	A, B, C, D	
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C, D	
Juvenile criminal records information	X	C, D	
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			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C, D	
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B	
- **User passwords/codes**	X	A, B	
- **IP address**	X	A, B	
- **Date/time of access**	X	A, B	

(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
- **Queries run**	X	A, B	
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	A, B	Some records may contain LEO names in the narrative section.

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		Email			
Other (specify):					

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)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
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	MIS information can only be accessed through a unique login to the system, given only upon user request and eligibility verification.
DOJ Components	X		X	Access to MIS is limited to members of partner agencies working on OCDETF cases or equities; each person's unique login access request is reviewed and approved prior to granting a MIS account and all access goes through DOJ intranet enabled workstation.
Federal entities	X		X	Access to MIS is limited to members of partner agencies working on OCDETF cases or equities; each person's unique login access request is reviewed and approved prior to granting a MIS account and all access goes through DOJ intranet enabled workstation.
State, local, tribal gov't entities	X		X	State and local personnel may have access to the information provided on the OCDETF MIS paper forms (which they submitted to OCDETF) for specific cases, but do not have any access, direct or otherwise, to the OCDETF MIS system itself.
Public	X			President's Budget Submission, which does not contain PII.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments	X			Restricted Access to investigative documentation for law enforcement. No OCDETF MIS access.
Foreign entities				None
Other (specify):				None

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.

N/A

Section 5: Notice, Consent, Access, and Amendment

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

Although individuals will have general notice of the existence of the system through the system of records notice and this PIA, targets of law enforcement investigations will not be provided individual notice. Notifying targets that information which pertains to them or their activities is collected, maintained, or disseminated by the system would risk circumvention of the law.

Individuals about whom related administrative records are kept, including information on state and local payments to state and local officers for state and local case participation is also maintained in the MIS system and is provided to OCDETF by the individuals themselves for budgetary reporting, auditing, and reconciliation purposes. These individuals are made aware that this information is collected, maintained and disseminated

by the MIS system because they are providing the information for the purpose of reimbursement tracking, and are provided a notice under Privacy Act subsection (e)(3). Similarly, contact information (i.e., name, phone number and email address) of case agents, case attorneys, and state and local personnel is also provided by the individuals themselves or their agencies for the known purpose of case tracking and coordination between agencies, and payment tracking for OCDETF state and local payments. MIS is covered by Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS) System of Records Notice, JUSTICE/OCDETF–001, 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), *available at* https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf.

MIS Privacy Act Notice:

Authority: 5 U.S.C. 301 and the Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91–513, 84 Stat. 1236 (21 U.S.C. 801 et seq.) authorize the collection of this information.

Purpose: Personal information collected on this form is used to make a determination on whether or not to grant the individual access to the MIS application, a Law Enforcement Sensitive system, and manage the user accounts.

Routine Uses: The information may be used by and disclosed (a) to any criminal, civil, or regulatory law enforcement authority (whether federal, state, local, territorial, tribal, or foreign) where the information is relevant to the recipient entity's law enforcement responsibilities; (b) to a governmental entity lawfully engaged in collecting law enforcement, law enforcement intelligence, or national security intelligence information for such purposes; and (c) to appropriate officials and employees of a federal agency or entity that requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the assignment, detail, or deployment of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant or benefit. Additionally, OCDETF may share this information in accordance with its published Privacy Act System of Records Notice (SORN) 78 FR 56737 (9-13-2013); 82 FR 24151, 160 (5-25-2017).

Disclosure: Providing the information on this form is voluntary; however, failure to furnish the requested information, may prevent or delay access to the MIS application.

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.

Investigative information is not gathered directly from individuals but from contributing agency records (and notice is not generally provided by the contributing agencies, and consent not requested, for the reasons in 5.1 and 5.3). Contributing agencies include contact information for law enforcement personnel and prosecutors assigned to each case.

This information is voluntarily submitted to the MIS by these individuals as part of the standard operating procedure for OCDETF cases on specific OCDETF MIS hard copy reporting forms via email to OCDETF Executive Office for review and data entry. Originating agencies are consulted prior to release of information for any purpose that is not explicitly described and agreed upon in each specific agency's memorandum of understanding (MOU) with OCDETF.

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.

Information about the individuals in this system is exempted from the notice, access and amendment provisions of the Privacy Act. Making this information subject to such rights risks circumvention of the law. *See* 28 C.F.R. § 16.135.

However, regarding information in the system about users of the system, individuals assigned to each case have real-time access to the information about themselves. These individuals, or the Agency responsible for submitting the information, may amend or correct the information at any time.

Insomuch as information submitted by agencies is responsive to a FOIA request, each applicable agency is consulted prior to release of such information.

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) (if the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced):** • ATO valid 9/23/2022 - 9/23/2025 **If an ATO has not been completed, but is underway, provide status or expected completion date:** N/A **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: N/A
	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: N/A
x	**This information or information 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 NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:** OCDETF MIS is categorized High Confidentiality, High Integrity, and High Availability, with an overall categorization of High. High Confidentiality: Data in MIS are open, active law enforcement investigations, the unauthorized disclosure of which could severe or catastrophic adverse impact on those investigations. High Integrity: Completed OFC work products incorporate data from OCDETF MIS. Unauthorized modification or destruction of the information would have severe or catastrophic adverse impact on the work products, and the law enforcement missions that these work products support, through incorrect or omitted information on targets of those law enforcement investigations. High Availability: Outages of OCDETF MIS and its components could cause severe or catastrophic adverse impact on the OCDETF mission.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Auditing is in place within the MIS operating environment and methods to consistently improve procedures are in place. Audit logs are reviewed as required by DOJ on a weekly basis. Audit logs are maintained for searching of defendants and prospective defendants. The ISSO and monitoring admins are responsible for review.
	Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:
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**.
	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:

	DOJ required Privacy Training is completed by all required system individuals. Although not privacy-specific, all administrators and users with data entry access are required to undergo a comprehensive training with an experienced OCDETF MIS trainer to ensure proper handling of information and data integrity prior to changing their role-based access control from "user" to "data entry".

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 OCDETF MIS is located in a secure facility on the secure DOJ Intranet network. OCDETF MIS is only accessible by machines authorized to connect to or within the DOJ Intranet. OCDETF MIS data is labeled as law enforcement sensitive throughout the OCDETF MIS. Access is controlled to mitigate risks from unauthorized access and misuse by authorized individuals. Additionally, access controls are in place to prevent unauthorized users from gaining access to the OCDETF MIS database (refer to Section 4.2 for further analysis).

Mandatory Training for Administrators and Users with Data Entry Access: All users are required to read and acknowledge an understanding of the Rules of Behavior and agree to follow them before using OCDETF IT resources. All users on any DOJ computer system, to include the OCDETF MIS, are required to complete the DOJ Cybersecurity Awareness training on an annual basis. That training covers "…DOJ security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act and DOJ Records Management Regulations…" DOJ personnel with access to personally identifiable information are also required to perform DOJ Privacy Training at onboarding.

Additionally, all administrators and all users with data entry access are required to undergo a comprehensive training with an experienced OCDETF MIS trainer to ensure proper handling of information and data integrity prior to changing their role-based access control from "user," with access limited to viewing information, to "data entry" with the ability to add, modify, and delete information. This training provides a variety of information on OCDETF guidance and processes. The training covers a review of the OCDETF MIS features, the OCDETF MIS forms, the form data fields; definitions of the form data fields; form approval processes; detailed demonstrations and hands on training for the addition and modification of MIS data as well as the proper handling of this data. This training also includes manual validation processes to ensure the integrity of data at the time of entry.

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.) If the project involves artificial intelligence and/or

machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.

OCDETF MIS data files have been deemed "Permanent" by NARA. A copy of the data maintained for each investigation is required to be transferred to NARA 25 years after the close of the case in accordance with 36 CFR 1228.270, or existing NARA-transfer requirements at the time of transfer. Paper copies are to be destroyed 5 years after the close of each case upon verification of successful conversion and input into the NARA system. OCDETF personnel work with appropriate records management contacts to ensure that data is maintained in accordance with records management requirements.

Additionally, privacy and security concerns of the systems are analyzed as part of the system's Assessment and Authorization (A&A) requirements, which are required as part of the application security controls under the National Institute of Standards and Technology (NIST) guidelines. The security of the information being passed on this connection is protected through the use of approved encryption mechanisms or Justice Unified Telecommunications Network (JUTNET)[1] certified approved mechanisms. Individual users will not have access to the data except through the DOJ Intranet. All users will sign the OCDETF Rules of Behavior for each account. Policy documents that govern the protection of the data are U.S. Department of Justice DOJ Order 0904 Cybersecurity Program, and applicable System Security and Privacy Plan (SSPP) with Authorization to Operate (ATO). Recognizing that access to priority target information should be limited for security and privacy reasons, the system was designed to limit access.

NARA Job Number N1-060-07-2
Inputs: Paper copies dated 1982 -Present
Temporary: Cut off data at the close of case. Destroy 5 years after cutoff upon verification of successful conversion and input into the system.

OCDETF MIS Data Files (Master File)
PERMANENT: Cut off data for closed cases annually. Transfer a copy of the data for closed cases to the National Archives and Records Administration 25 years after cutoff, in accordance with 36 CFR 1228.270, or existing NARA-transfer requirements at the time of transfer.

[1] JUTNET is covered by separate privacy documentation.

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:

System Number: JUSTICE/OCDETF-001
System Name: Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS)
Federal Register: 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), *available at* https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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,***
- ***Type of technology employed (e.g. AI/ML),***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

The OCDETF MIS implements security and privacy administrative and physical

safeguards/controls to reduce the risk to compromise PII information. Access to information within these applications are need-to-know only. Role-based access controls are enforced to restrict access, and privileged access is assigned to only a few system administrators. Only a small number of personnel have direct access to all data in the OCDETF MIS system. The only people who qualify for such access are a small number of OCDETF technical employees with appropriate background investigations. These technical employees can only use this access in a DOJ controlled facility and hosted platform.

All federal agents, attorneys, and analysts, who are the core users of the OCDETF MIS, must have a positively adjudicated background investigation qualifying them for a clearance to access Secret-level national security information, are required to agree to the rules of behavior for OCDETF MIS access, must take cyber security awareness training within their agencies, and receive OCDETF MIS training throughout the year from OCDETF. OCDETF also audits the information collected to ensure consistency in the information and that information is complete and correct (such as correct names and dates, fixing typos, and resolving incomplete information) to ensure proper reporting.[2] When issues are identified, additional training is provided.

A second layer of protection is provided by virtue of the design and implementation of the OCDETF MIS application. Moreover, OCDETF MIS users are made aware of the ramifications of revealing the OCDETF MIS information to unauthorized individuals by the rules of behavior to which they must agree and the system-provided warning banner. Penalties for such behaviors range from suspensions to firings to prison sentences.

Access to individual records is gained by use of data retrieval capabilities of computer software acquired and developed for processing of information in the OCDETF MIS. Data is retrieved predominately by case number but can also be retrieved through a number of criteria, including personally identifying information such as name and social security number. OCDETF shares information with participating federal and state and local entities. However, state and local agencies do not have access to the OCDETF MIS system. Federal, state, and local agencies that work with OCDETF but are not system users may request information from authorized users on a case-by-case basis, as necessary based on their role in the investigation. System users seeking to share OCDETF information with third parties must first clear the request through the OCDETF Executive Office. Non-DOJ employees that are detailed to the OCDETF Program, and are located in DOJ facilities, may request to obtain DOJ network access in order to access the OCDETF database.

Mitigation of Misuse by Authorized Individuals: OCDETF determines user access of information for all OCDETF MIS account users. For authenticated users, access is controlled through role-based permissions at the group level and at the user level, as

[2] 3 As stated in Section 1, above, OCDETF provides various reports periodically to the President, the Attorney General, the Congress, and the public.

required. Not all users have the ability to edit or change data within the system. Only those users trained and assigned a data entry role have the ability to edit or change data in the system.

Additionally, the following User Certification is included on the Account Request Form and must be certified by the requester when applying for an OCDETF MIS account.

> *User Certification: I understand that the OCDETF MIS contains Law Enforcement Sensitive Information and that the information contained in and the reports generated from the OCDETF MIS must be protected and not released to unauthorized individuals. I have read and agree to abide by the rules of behavior established by the U.S. Department of Justice/OCDETF for system use. By signing below, I understand that I am responsible for ensuring that OCDETF MIS information is not improperly disseminated or disclosed. I acknowledge that unauthorized disclosure may result in prosecution for obstruction of justice, misuse of government property or another appropriate charge.*

Audit logs are maintained to capture certain actions, queries, and search terms, within the OCDETF MIS. OCDETF reviews audit logs on at least a weekly basis. User accounts are reviewed on a rolling basis as OCDETF is notified of departing users but will also be formally reviewed during the annual review, at the same time that the audit logs are reviewed.

Mitigation of Unauthorized Access: The OCDETF MIS access request process was designed to protect the sensitive personal information of targets, prospective targets, case agents, case attorneys and state and local officers contained therein. Although all users have access to personally identifiable information maintained by the system, access to that information is restricted to users who have undergone background investigations, are cleared,[3] and are required to have several approvals prior to being granted access and trained on the system.

Those persons who are authorized for OCDETF MIS accounts must be appropriately cleared for such access by the users' home agency and by OCDETF Security prior to obtaining OCDETF MIS access. Contractor personnel performing hardware installation or maintenance must be similarly cleared for access by OCDETF Security or escorted at all times by appropriately cleared and knowledgeable OCDETF employees. After the background investigation has been completed, or a waiver of the completion of an initiated background investigation has been approved, a user's immediate supervisor may submit system access requests to the system administrator. Therefore, the process to gain access ensures that only authorized individuals are granted access to the information maintained

[3] OCDETF MIS requires a background investigation clearing the individual for access to SECRET level national security information, although the actual clearance is not necessary for access because OCDETF MIS information is not national security information.

by the OCDETF MIS. User access to the OCDETF MIS is restricted at the operating system and application levels. Users are granted access only to the data required to complete their assigned duties.

Although OCDETF is normally notified of departing OCDETF MIS users, the OCDETF Executive Office sends out annual requests to agency partners asking each to update the user list pertaining to their specific agency to further ensure the accuracy of the account status of OCDETF MIS users within the system. However, while requests are sent annually, the system is continuously monitored for locked accounts and security conducts ongoing audits to ensure that appropriate clearances are maintained. Agency partners have 90 days to respond to the OCDETF requests for updated user lists. If an agency partner does not timely confirm the accuracy of its user list, all user accounts on that list will be deactivated. Once an account is deactivated, the agency partner must submit a new request to obtain OCDETF MIS access.

Additionally, all passwords expire after 60 days. Upon password expiration, a system administrator must be contacted in order to renew the password. Prior to renewing any password after expiration, the OCDETF MIS system administrator is required to contact the password user's specific agency to confirm the propriety of such user's access renewal. If the user's account is deactivated, the user is required to re-apply for access to the system. Users can also renew their passwords prior to the 60-day expiration. However, all accounts are reviewed annually regardless of password expiration. All users are required to read and acknowledge understanding of the Rules of Behavior before using OCDETF IT resources.

General notice of the system of records is provided to the public in the Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS) System of Records Notice, JUSTICE/OCDETF–001, 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), available at https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf.