Executive Office for the Organized Crime Drug Enforcement Task Forces

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

Issued by:

Kristin D. Brudy-Everett
Acting Senior Component Official for Privacy
Executive Office for OCDETF
Department of Justice
202-616-1931

Reviewed by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
Department of Justice

Date approved: March 7, 2022

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.)

OCDETF Management Information System (MIS):

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 1(d) 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 enable OCDETF management and personnel to review and evaluate investigative efforts.

OCDETF High Intensity Drug Trafficking Area (HIDTA) Parcel Interdiction Portal (PIP:

The HIDTA Parcel Interdiction Portal (HIDTA PIP) is a web-based law enforcement investigative tool/application that is hosted on the Department of Justice (DOJ) Service Delivery Staff (SDS) Azure Linux environment. The project operates pursuant to Memorandum of Understanding (MOU) between DOJ OCDETF and Appalachian HIDTA (AHIDTA). As the centerpiece of the DOJ counter-narcotics strategy, OCDETF is authorized to enter into this MOU pursuant to 21 U.S.C. § 873, which vests the Attorney General with the authority to arrange for the exchange of information between governmental officials concerning the use and abuse of controlled substances. HIDTA PIP application is focused towards information sharing among different law enforcement agencies pertaining to parcel interdiction in order to reduce drug trafficking. The content represented in the application consists of information, including information in identifiable form, regarding parcel seizures of drugs and currency provided by federal, state, tribal and local law enforcement agencies. Information elements in the application are: parcel location, recipient and sender addresses, type of drugs or currency seized, and department or agency that seized it. Phone numbers used when shipping packages may also be collected if available, but these may or may not be associated with a particular person (and considering the nature of the name of sender or recipient and a phone number may not be legitimate/real). Provided information is entered within the application by authorized system administrators and parcel editors. Agents and officers can use this application data for informational purposes[1] and lead development only. The application also collects certain information from individuals as part of a user accounts registration, vetting, and creation process (i.e., name, agency, contact information, title, and supervisor information). Collection and use of PII associated with the account request process are provided and entered within the system by the local, state, tribal, and federal law enforcement agents and analyst requiring access to the application. This data can be only updated by such individuals themselves or system administrators if needed.

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

[1] As used in this PIA, "informational purposes" means it is incumbent on the individual receiving this information to develop their own investigative techniques to further their investigation. HIDTA PIP information is not to be incorporated into affidavits, court proceedings, or case files. It is provided strictly for leads information. Each agency must develop their own probable cause to justify obtaining arrest and/or search warrants. Any activities resulting from information retrieved from within PIP must be deconflicted independently by the user. PIP is not a deconfliction system, and does not certify any level of deconfliction has taken place. HIDTA PIP information only indicates that a package was intercepted in transit from one stated location to another.

activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

OCDETF Management Information System (MIS):

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 in a position to disrupt and dismantle sophisticated drug and money laundering organizations alone. OCDETF combines the resources and expertise of its eleven federal agency members ─ the 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.

OCDETF High Intensity Drug Trafficking Area (HIDTA) Parcel Interdiction Portal (PIP):

HIDTA PIP is a web-based law enforcement investigative tool pertaining to parcel interdiction that provides assistance to federal, state, local, and tribal law enforcement agencies through information sharing, with the goal of reducing drug trafficking. The application collects, maintains, and stores information pertaining to drugs and currency parcel interdiction. It includes only parcel location, recipient and sender addresses, type of drugs or currency seized, and department or agency that seized it. Phone numbers used when shipping packages may also be collected if available, but these may or may not be associated with a particular person (and considering the nature of the name of sender or recipient and a phone number may not be legitimate/real). This information is entered within the application by a parcel editor associated with the agency that seized the parcels or by the HIDTA administrators once data is received from the participating agencies. Agents and analysts with authorized application accounts can use this data for informational purposes and lead development only. The application also collects certain information from individuals as part of a user accounts registration, vetting, and creation process (i.e., applicant email address, username, first and last name, title/rank, parent agency, agency type, county, state, work cell number, email, supervisor first/last name, title/rank, phone number and email). Collection and use of PII associated with the account request process are provided and entered within the system by the local, state, tribal, and federal law enforcement agents and analyst requiring access to the application. This data can be only updated by such individuals themselves or system administrators if needed.

All users are vetted and verified by the HIDTA administrator based on required registration information. All users are assigned permissions based on approved roles within the application and access the application using unique identifier and authenticators managed within the application. Most users are assigned law enforcement role/access which provides the most basic user account level, limited to the ability to query the system for parcels, and save searches. Ability to manage system accounts is provided only to few system administrators. Parcel Editors role is authorized for a small number of users that have been granted permission to submit parcels information to the system. Only one system developer/task force officer manages the application and database settings and development. This system task force officer has a direct access to the DOJ network and supporting SDS Azure platform server. This access is done through DOJ implemented remote access, using DOJ provided account, laptop and DOJ employed multifactor authentication (MFA).

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	These records are maintained pursuant to 5 U.S.C. 301 and 21 U.S.C. 841 and 873. Consolidated Appropriations Act, 2004, Public Law 108-199, 118 Stat. 3 (2004) Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91–513 (84 Stat. 1236)
Executive Order	E.O. 11396
Federal Regulation	
Agreement, memorandum of understanding, or other documented arrangement	Memorandum of Understanding (MOU) between DOJ OCDETF and Appalachian HIDTA
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.

(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, D	HIDTA PIP/MIS
Date of birth or age	X	A, B, C, D	MIS only
Place of birth	X	A, B, C, D	MIS only
Gender	X	A, B, C, D	MIS only
Race, ethnicity or citizenship	X	A, B, C, D	MIS only
Religion			
Social Security Number	X	C	MIS only
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C, D	MIS only

Passport number			
Mother's maiden name			
Vehicle identifiers	X	C, D	MIS only
Personal mailing address	X	MIS: A, B, C, D HIDTA PIP: (C, D) home address of the sender and recipient.	MIS HIDTA PIP: This information may be fictitious.
Personal e-mail address		A, B, C, D	MIS
Personal phone number		A, B, C, D	MIS/HIDTA PIP (Note: HIDTA PIP (A, B) system may collect personal/cell phone number associated with system users and supervisors. In addition, system may contain parcel sender and receiver phone number (C, D), but this information may be fictitious.)
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	X	A, B	HIDTA PIP: HIDTA PIP may possibly collect rank information on DOJ and Federal Government individuals that have access to the HIDTA PIP application as part of application account creation. In addition, employment/business information such as work agency (federal, local, state or tribal), work email, supervisor first and last name, including work phone number and email may be collected.
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	MIS only
Juvenile criminal records information	X	C, D	MIS only
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	X	C, D	MIS only
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	MIS only
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	MIS/HIDTA PIP
User passwords/codes	X	A, B	MIS/HIDTA PIP
IP address			
Date/time of access	X	A, B	MIS/HIDTA PIP
Queries run	X	A, B	MIS/HIDTA PIP
Content of files accessed/reviewed			
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.

General explanation regarding chart content above:

Regarding PIP, there are no free-text fields allowing users to enter unexpected or unrequested information content. Regarding MIS, the particular information fields have validated structures; however, there is a narrative section with very specific questions where free text responses are allowed. Thus, for MIS, the indications in the chart above reflect information foreseeably collected, although it is possible that users may enter other information using the free text capability. Users are advised in training that they should only enter information specifically requested.

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

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	X
Telephone		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):	X	Informants and Interested Third Parties			

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-Case	Bulk Transfer	Direct access	Other (specify)
Within the component	X		X	MIS/HIDTA PIP
DOJ components	X		X	MIS/HIDTA PIP
Federal entities	X		X	MIS: Access to DOJ Intranet enabled workstation must be granted prior to granting access to the OCDETF MIS. HIDTA PIP: HIDTA PIP application is web based and available on the internet to approved and authorized federal law enforcement agents and analysts. They only have access to the application's drug and currency parcels data based on their authorized access (end user/law enforcement or parcel editor role).
State, local, tribal gov't entities	X		X	MIS: 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. HIDTA PIP application is web based and available on the internet to approved and authorized local, state, and tribal law enforcement agents and analysts. They only have access to the application's drug and currency parcels data based on their authorized access (end user/law enforcement or parcel editor role).
Public	X			President's Budget Submission, which does not contain PII
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				No disclosures to non-government attorneys or non-law enforcement officer witnesses.
Private sector				None
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.

Not applicable.

Section 5: Notice, Consent, 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.

OCDETF MIS: 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 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). HIDTA PIP: The HIDTA PIP information is covered by 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).

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.

HIDTA PIP Privacy Act Notice (The "create new account" page contains a notice required by subsection (e)(3) of the Privacy Act.):

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 HIDTA PIP application, a Law Enforcement Sensitive system, as well as manage user accounts.

Routine Uses: The information will 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, HIDTA PIP 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 HIDTA PIP 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.

OCDETF MIS: 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.[2] 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.

[2] Very specific OCDETF MIS reporting forms must be submitted throughout the investigation until closure in order to ensure that investigations rise to the appropriate level for OCDETF designation and maintain that status.

HIDTA PIP: PII associated with the account request process (name, work email, phone number, supervisor name, work email and phone number) is provided and entered within the system by the local, state, tribal, and federal law enforcement agents and analysts requiring access to the application. This data can be updated by the agents and analysts themselves. Parcel and currency seizure data associated is not gathered directly from individuals but from contributing agencies that seized the parcels. No opportunity is provided for individuals to voluntarily participate in collection, use, or dissemination of parcel and currency seizure data because such participation would risk compromising investigations.

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.

In the event that 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):** OCDETF MIS 09/30/2019; HIDTA PIP 05/19/2021 **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:**
	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:** The security and privacy controls listed in the MIS and HIDTA PIP System Security and Privacy Plan have been assessed to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. This is part of a continuing monitoring program that is in place within the MIS and HIDTA PIP operating environment. The OCDETF MIS maintains PII for prospective defendants, defendants, case attorneys, case agents, and OCDETF MIS users. MIS and HIDTA PIP security and privacy controls are assessed annually or as required more often based on system changes and updates. The vulnerability scans are performed on a monthly basis.
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:** Auditing is in place within the MIS and HIDTA PIP operating environment and methods to consistently improve procedures are in place. Audit logs are reviewed as required by DOJ on a weekly basis. In addition, HIDTA PIP system is monitored by DOJ enterprise monitoring tool Splunk/SIEM. Audit logs are maintained for searching of defendants and prospective defendants. The ISSO and monitoring admins are responsible for review.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy.**
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** 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?

OCDETF Management Information System (MIS):

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 on an annual basis the DOJ Cybersecurity Awareness training. 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.

OCDETF High Intensity Drug Trafficking Area (HIDTA) Parcel Interdiction Portal (PIP):

The HIDTA PIP application is hosted within secure and authorized U.S. Department of Justice (DOJ) Service Delivery Staff (SDS) Azure platform and operated by SDS within the Justice Management Division (JMD). The HIDTA PIP application is web based and available on the internet to approved and authorized system users from federal, state, local, and tribal law enforcement agencies. All users are vetted and verified by the HIDTA administrator based on required registration information. Users are assigned permissions based on approved roles within the application and access the application using unique identifier and authenticators managed with the application. Web application is accessed and all data transmitted through secure FIPS 140-2 compliant and approved. Most users are assigned a law enforcement role/access which provides the basic user account level and is limited to querying the system for information about seized parcels, saving results of searches. Ability to manage system user accounts is provided only to a few system administrators, with restricted privileged access based on their role. Parcel Editors role is authorized for a small number of users that have been granted permission to submit parcels information to the system. Only one system developer, who is a task force officer, has a direct access to the DOJ network and supporting SDS Azure server to manage the application and database. This access is done through DOJ implemented remote access, using DOJ provided account, laptop and DOJ employed multifactor authentication (MFA). All user actions including privileged user actions are logged and audited and logs are reviewed by the system administrators at least weekly.

HIDTA PIP application is designed to the extent feasible to support privacy by automating privacy controls. Privacy controls are built and included in the application system design and development in accordance with DOJ security and privacy policies to mitigate privacy risks, including breaches and incidents. Collection and use of PII associated with the account request process are provided and entered within the system by the local, state, tribal, and federal law enforcement agents and analyst requiring access to the application. This data can only be updated by such individuals themselves or system administrators if needed.

Data associated with the parcel seizure is entered within the application by the parcel editor associated with the agency that seized the parcels or by the HIDTA administrators once data is received from the participating agencies. This data can be updated and deleted within the system only by these authorized personnel. Authorized local, tribal, state and federal law enforcement and analysts can use the application for informational purposes and lead development only. All user action including data usage is audited

and logged by the system and reviewed on at least weekly basis. Data is retained within the system as long as needed in accordance with DOJ Cybersecurity and NARA requirements. PII is disclosed in accordance with DOJ defined privacy process and privacy notices including this PIA and the JUSTICE/OCDETF–001 SORN, and consistent with the DOJ OCDETF/AHIDTA MOU. In accordance with DOJ/HIDTA MOU, users are not allowed to publish or otherwise reveal HIDTA information to third parties without the written permission of the party that initially entered the information into the HIDTA PIP.

HIDTA PIP personnel with security roles such as System Owner, System Security and Privacy Officer, Authorizing Official, etc., including system task officer and administrators and DOJ HIDTA users are also required to complete DOJ Cyber Security Awareness Training (CSAT) on at least an annual basis or more often based on system changes. In addition, DOJ Privacy Training is completed annually by all HIDTA PIP administrators, system task force officer and individuals with assigned privacy roles. HIDTA PIP/OCDETF monitors, audits, and trains its staff on the authorized sharing of PII and on the consequences of unauthorized use or sharing of PII. HIDTA PIP data is only shared in accordance with the AHIDTA MOU and documented privacy clause. All participating agencies have agreements with AHIDTA that contain privacy clauses and are bound by such agreement on the data sharing. These agencies also provide privacy training to their employees. In addition, the application login page contains rules of behavior for all system users that provide information on proper handling of the system and its data including PII information.

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.)

Data Retention & Disposal: 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 JUTNET certified approved mechanisms. Individual users will not have access to the data except through the DOJ Intranet. All DOJ users will sign the OCDETF Rules of Behavior (ROB) for each account. Policy documents that govern the protection of the data are U.S. Department of Justice DOJ 2640.2F, and applicable System Security and Privacy Plan (SSPP) with Approval 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.

HIDTA PIP retains and dispose data in accordance with NARA requirements.

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.

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), last updated 82 Fed. Reg. 24151, 160 (May 25, 2017)

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- **Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),**
- **Sources of the information,**
- **Specific uses or sharing,**
- **Privacy notices to individuals, and**
- **Decisions concerning security and privacy administrative, technical and physical controls over the information.**

The OCDETF MIS and HIDTA PIP implement 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 few system administrators. Only a small number of personnel have

direct access to all data in the OCDETF MIS and HIDTA PIP systems. 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.[3] 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 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*

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

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,[4] 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 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

[4] 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.

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.

OCDETF High Intensity Drug Trafficking Area (HIDTA) Parcel Interdiction Portal (PIP):

HIDTA PIP uses minimal personally identifiable information (PII) elements/data necessary to accomplish the legally authorized purpose, system function and mission in accordance with the AHIDTA/OCDETF Memorandum of Understanding (MOU). This along with the implementation of all required and current National Institute of Standards and Technology (NIST) Special Publication 800-53 security and privacy controls through the system development lifecycle and risk management framework minimizes privacy risk associated with the PII data usage. Application functionality is focused towards information sharing among different law enforcement agencies pertaining to parcel interdiction in order to disrupt and dismantle drug trafficking. Authorized agents and officers can use the data within the application for informational purposes and lead development only as stated in the application website legal notice. Parcel interdiction data is collected by the local, state, tribal and federal agencies and provided and/or entered within the application by the HIDTA administrators or agency assigned parcel editors. Only the following PII information is required to be collected: "To" address (country, street, city, zip code state). Additional info such as first and last name on "To" and "From" address could be entered if available. "From"/ "Sender" phone number can be entered if available but is not necessary to accomplish the legally authorized purpose of collection. This Parcel interdiction PII data can only be accessed and modified by the authorized individuals such as system administrator or parcel editor who has entered the specific agency parcel data.

As part of the account request process through the application "create new account" webpage, the following PII data is collected for the purpose of vetting applicants and approving accounts: email address, username, first and last name, title/rank, parent agency, agency type, county, state, work cell number, email, supervisor first/last name, title/rank, phone number and email. The HIDTA PIP Privacy Act Notice is displayed on this page – the text of which is covered in Section 5 of this document, above.

PII data associated with the user registration is provided directly by the law enforcement agents and analysts requiring access to the system. This data can only be modified/updated by the requesting users/account owners themselves or by the system administrators.

As noted above, HIDTA PIP PII data can only be accessed by authorized individuals through the implementation of role-based access. Only required minimal permissions are assigned for the users to be able to perform their assigned roles as documented in section 6.2 above. HIDTA PIP end users only have access to application data based on their role and are required to indicate acceptance to statements on a warning banner and legal notice before further access to the application is allowed. All user actions including privileged user actions are logged and audited and logs are reviewed by the system administrators at least weekly. All users are made aware of legal ramification associated with system misuse by notification of the application login page warning banner which clearly states that the information system is provided for authorized use only and unauthorized or improper use of the system may result in disciplinary action, and civil and criminal penalties. All authorized user accounts are reviewed annually by the system administrators to validate access authorization including active and disabled accounts. User accounts are also disabled after 90 days of inactivity and when system

administrators are notified that accounts are no longer needed. Integrity and confidentiality of the application data including PII is provided by the implementation of secure encryption mechanism.

General notice of the system of records is provided to the public in the following OCDETF SORN: 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), last updated 82 Fed. Reg. 24151, 160 (May 25, 2017) which covers HIDTA PIP information.

HIDTA PIP will also evaluate and review PII holdings identified in the PIA on an annual basis to ensure that only PII identified in the PIA is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. Reviews may be done more often due to application changes that may impact PII or any changes in PII collection and processing. If PII holding changes, a security and privacy impact and risk analysis will be performed and if required additional controls and needed enhancements will be implemented to ensure adequate system security.