

# Executive Office for the Organized Crime Drug Enforcement Task Forces



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

---

**Issued by:**

**Jill Aronica**  
Chief, Information System Section/Component Privacy POC  
Executive Office for OCDETF  
Department of Justice  
202-514-1860

**Kenneth Courter**  
Acting Senior Component Official for Privacy  
Executive Office for OCDETF  
Department of Justice  
202-514-1860

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

Date approved: April 1, 2020

*(May 2019 DOJ PIA Template)*

## **Section 1: Executive Summary**

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

The 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 its 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. 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.

## **Section 2: Purpose and Use of the Information Technology**

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

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 civil 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 report case 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.

## **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.  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	
	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	
Date of birth or age	X	A, B, C, D	
Place of birth	X	C, D	
Gender	X	C, D	
Race, ethnicity or citizenship	X	C, D	
Religion			
Social Security Number	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	C, D	

<b>Personal e-mail address</b>			
<b>Personal phone number</b>		C, D	
<b>Medical records number</b>			
<b>Medical notes or other medical or health information</b>			
<b>Financial account information</b>			
<b>Applicant information</b>			
<b>Education records</b>			
<b>Military status or other information</b>			
<b>Employment status, history, or similar information</b>			
<b>Employment performance ratings or other performance information, e.g., performance improvement plan</b>			
<b>Certificates</b>			
<b>Legal documents</b>			
<b>Device identifiers, e.g., mobile devices</b>			
<b>Web uniform resource locator(s)</b>			
<b>Foreign activities</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
<b>Criminal records information, e.g., criminal history, arrests, criminal charges</b>	X	C, D	
<b>Juvenile criminal records information</b>	X	C, D	
<b>Civil law enforcement information, e.g., allegations of civil law violations</b>			
<b>Whistleblower, e.g., tip, complaint or referral</b>			
<b>Grand jury information</b>			
<b>Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information</b>	X	C, D	
<b>Procurement/contracting records</b>			
<b>Proprietary or business information</b>			
<b>Location information, including continuous or intermittent location tracking capabilities</b>			
<b>Biometric data:</b>			
<b>Photographs or photographic identifiers</b>	X	C, D	

<b>Video containing biometric data</b>			
<b>Fingerprints</b>			
<b>Palm prints</b>			
<b>Iris image</b>			
<b>Dental profile</b>			
<b>Voice recording/signatures</b>			
<b>Scars, marks, tattoos</b>			
<b>Vascular scan, e.g., Palm or finger vein biometric data</b>			
<b>DNA profiles</b>			
<b>Other (specify)</b>			
<b>System admin/audit data:</b>			
<b>User ID</b>	X	A, B	
<b>User passwords/codes</b>	X	A, B	
<b>IP address</b>			
<b>Date/time of access</b>	X	A, B	
<b>Queries run</b>	X	A, B	
<b>Content of files accessed/reviewed</b>			
<b>Contents of files</b>			
<b>Other (please list the type of info and describe as completely as possible):</b>			

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

<b>Directly from individual about whom the information pertains</b>					
In person		Hard copy: mail/fax		Online	
Telephone		Email			
Other (specify):					

<b>Government sources</b>					
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):					

<b>Non-government sources</b>					
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			Restricted Access. Access controls are described in Section 4.2.
DOJ components	X			Restricted Access. Access controls are described in Section 4.2.
Federal entities	X			Restricted Access. Access to DOJ Intranet enabled workstation must be granted prior to granting access to the OCDETF MIS.
State, local, tribal gov't entities	X			Restricted Access to investigative documentation only. No OCDETF MIS access.
Public	X			President's Budget Submission
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.**

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 is collected, maintained or disseminated by the system which pertains to them or their activities would risk circumvention of the law.

Individuals for which 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 system are provided by the individuals themselves for reporting purposes. These individuals are aware that this information is collected,

maintained and disseminated by the system. 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. No additional notice is provided, consistent with exemption taken to 5 USC 552a(e)(3). See 28 C.F.R. § 16.135.

**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 individuals assigned to each case. This information is voluntarily submitted through the reporting process and 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).

**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.**

The individuals for which data is collected are targets of law enforcement investigations; and therefore these individuals do not have the opportunity to consent to particular uses of the information. Notifying them that information is collected, maintained or disseminated by the system which pertains to them or their activities would risk circumvention of the law. Procedures for requesting access to and amendment of MIS Privacy Act records are outlined in the system of records notice JUSTICE/OCDETF-001, 78 FR 56738 (Sept. 13, 2013).

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).**

<input checked="" type="checkbox"/>	<p><b>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):</b>   09/30/2019  </p> <p><b>If an ATO has not been completed, but is underway, provide status or expected completion date:</b>   N/A  </p> <p><b>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:</b></p>
	<p><b>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:</b></p>
<input checked="" type="checkbox"/>	<p><b>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</b></p> <p>The security controls listed in the System Security 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.</p> <p>This is part of a continuing monitoring program that is in place within the MIS operating environment. The OCDETF MIS maintains PII for prospective defendants, defendants, case attorneys, case agents, and OCDETF MIS users. The security controls are assessed annually or as required. The vulnerability scans will be performed quarterly.</p>
<input checked="" type="checkbox"/>	<p><b>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</b></p> <p>Auditing is in place within the MIS operating environment and methods to consistently improve procedures are in place. Audit logs are maintained for searching of defendants and prospective defendants. The ISSO is responsible for review. The logs are reviewed quarterly.</p>
<input checked="" type="checkbox"/>	<p><b>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.</b></p>
<input checked="" type="checkbox"/>	<p><b>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:</b> 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”.</p>

**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, only accessible to 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 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 Computer Security 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..."

Additionally, 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". 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.)

**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 system are analyzed as part of the system's Certification and Accreditation (C&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 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 Plan (SSP) 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.

NARA Job Number N1-060-07-2

1. 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.

2. 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.  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 FR 56737 (Sept. 13, 2013)

**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 implements technical security to reduce the risk to compromise PII information. Access to the system is based on need-to-know. The system enforces role based access controls to restrict access. Only a small number of technical employees with appropriate background investigations have access to the system in a controlled facility.

The agents, attorneys, and analysts who are the core users of the OCDETF MIS are trained to understand the legal restrictions that govern their use of the information with which they are entrusted. This training starts with their entrance into government service and continues with periodic refreshers throughout their careers.

A second layer of protection is provided by virtue of the design and implementation of the OCDETF MIS application. Moreover, OCDETF MIS users are fully aware of the personal, career and legal ramifications of revealing the OCDETF MIS information to unauthorized individuals. 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. Non-DOJ partnering agencies, and State and local agencies, may request information from authorized users on a case-by-case basis, as required or necessary by their role in the investigation. Federal 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 any 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 and requests on a quarterly basis. User accounts are reviewed on a rolling basis as OCDETF is notified of departing users, but will also be formally reviewed with 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, and are required to have several approvals prior to being granted access and trained on the system.

Those authorized OCDETF MIS accounts must be appropriately cleared. Contractor personnel performing hardware installation or maintenance must be similarly cleared 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 level required to complete their assigned duties.

Although OCDETF is normally notified of departing OCDETF MIS users, the OCDETF Executive Office sends out regular 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. In the unlikely event a departing OCDETF MIS user is overlooked, all passwords expire within a set amount of time and a system administrator must be contacted in order to renew the password which automatically requires the administrator to check on the status of the user's account during the process of password renewal. If the user's account is in "Inactive" status, the user is required to re-apply for access to the system.

All users are required to read and acknowledge understanding of the Rules of Behavior before using OCDETF IT resources.