

Executive Office for the



Organized Crime Drug Enforcement Task Forces

Privacy Impact Assessment for Oak Island

Issued by:

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

Reviewed by:

Andrew McFarland
Senior Counsel
Office of Privacy and Civil Liberties
Department of Justice

Date approved:

December 13, 2024

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

The OCDETF Fusion Center (OFC) is the cornerstone of OCDETF's intelligence efforts. The OFC significantly enhances OCDETF's overall capacity to engage in intelligence-driven, coordinated law enforcement. The OFC is a comprehensive data warehouse containing drug and related financial intelligence information from OCDETF member investigative agencies, the Treasury Department's Financial Crimes Enforcement Network (FinCEN), as well as relevant data from additional federal and international agencies and partner organizations.

The OCDETF Management Information System (MIS)¹ 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.

Oak Island is a FISMA-non reportable system and it is categorized as Moderate in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Information Systems. Oak Island does not store any personally identifiable information (PII) data with the exception of system admin/audit data as noted in the table below, as well as possibly in the system development space.

¹The OCDETF Management Information System (MIS) is covered by separate privacy documentation available here: <https://www.justice.gov/opcl/doj-privacy-impact-assessments>

Oak Island provides Internet access to users from multiple federal agencies and contractors at the OCDETF Fusion Center; these users utilize Oak Island to conduct open source and related checks (e.g. Lexis/Nexis, Dunn & Bradstreet, etc.) and to perform anonymized searches of information available on the Internet. Oak Island also supports downloads of necessary system patches and updates and for remote system maintenance by the IT Support section, and by software developers to perform application development and testing for software used by the OCDETF Fusion Center on other accredited networks.

In accordance with the E-Government Act of 2002, OCDETF prepared this privacy impact assessment because Oak Island may contain limited amounts of PII in “test” data (often fake mock-up data, but there are possibly real records as well).

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.

Oak Island provides system development, management, maintenance, and mission support infrastructure for OCDETF and OCDETF Fusion Center, including the Fusion Desktop application². Fusion Desktop information includes investigative case information from member federal law enforcement agencies and partners as well as information covered by the Bank Secrecy Act (BSA).

Oak Island collects and maintains only such information as is necessary to monitor usage of the network (e.g., system and audit logs of user activity). However, as Oak Island may be used for software development for the OCDETF MIS and the OCDETF Fusion Center systems such as Fusion Desktop, it may contain limited amounts of PII in “test” data (often fake mock-up data, but there are possibly real records as well).

The Fusion Desktop’s data warehouse is made up of that investigative case information, Financial Crimes Enforcement Network (FinCEN) bulk data, and Department of State visa application holdings. OFC Products contain excerpted data from those sources, including both PII of subjects of active criminal investigations as well as PII of associated federal law enforcement personnel (such as case agent names and contact information). Records may contain investigative and intelligence information about the individuals in this system, including their identifying information such as, but not limited to, name, date of birth, gender, social security number, address, physical description, photograph, operator license (e.g., driver, airman, mariner), international travel information (e.g., visa adjudication, issuance, and refusal information, country of citizenship, travel documents, admission and departure processing), vehicle license plate/number and other information on conveyances used, bank account number, location/activities, as well as other data which may assist the OFC in fulfilling its responsibilities

² Fusion Desktop Application is covered by separate privacy documentation available here:
<https://www.justice.gov/opcl/doj-privacy-impact-assessments>.

and/or OCDETF's International Organized Crime Intelligence and Operations Center (IOC-2) in fulfilling its responsibilities. Information includes multi-source data that may assist law enforcement agencies, regulatory agencies, and agencies of the U.S. foreign intelligence community or military community in executing their responsibilities with respect to drug trafficking, international organized crime, money laundering, firearms trafficking, alien smuggling, terrorism, and other enforcement efforts, including the identification, location, arrest and prosecution of suspects, and civil proceedings and other activities related to such enforcement activities.

Finally, Oak Island maintains PII on its end users for auditing purposes to include name, official email, and phone numbers.

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

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

2.2 *Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)*

Authority	Citation/Reference
Statute	<ul style="list-style-type: none"> - Title 21 U.S.C § 878, Controlled Substance Act - Title 18 U.S.C § 2518, (1) (e), Crimes and Criminal Procedures - Consolidated Appropriations Act, 2004, Public Law 108–199, 118 Stat. 3 - Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91– 513, 84 Stat. 1236 (21 U.S.C. § 801 <i>et seq.</i>) - Organized Crime Control Act of 1970, Public Law 91–452, 84 Stat. 922
Executive Order	<ul style="list-style-type: none"> - Executive Order 11396, 33 Fed. Reg. 2689 (1968), 3 C.F.R. 1966-1970 Com0p. p. 711.
Federal regulation	<i>See id.</i>

Agreement, memorandum of understanding, or other documented arrangement	<ul style="list-style-type: none"> - United Nations Single Convention on Narcotic Drugs, 1961 - United Nations Convention on Transnational Organized Crime, 2000
Other (summarize and provide copy of relevant portion)	Additional authority is derived from Treaties, Statutes, Executive Orders, and Presidential Proclamations which DOJ has been charged with administering.

Section 3: Information in the Information Technology

3.1 *Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2) and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Name:	X	A, B, C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include names of targets of investigations and their associates as well as members of the public (US and non-USPERs), and names of investigative personnel including case agents and federal attorneys, included through source data.</p>
Date of birth or age	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Place of birth	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include includes other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Gender	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Race, ethnicity, or citizenship	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Religion	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop and MIS include includes SSNs of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Tax Identification Number (TIN)	X	C, D	Fusion Desktop includes government assigned identifiers to include passport, alien ID, tax ID, drivers' licenses, etc., of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings and visa applications.
Driver's license	X	C, D	Fusion Desktop includes government assigned identifiers to include passport, alien ID, tax ID, drivers' licenses, etc., of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings and visa applications.
Alien registration number	X	C, D	Fusion Desktop includes government assigned identifiers to include passport, alien ID, tax ID, drivers' licenses, etc., of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings and visa applications.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Passport number	X	C, D	Fusion Desktop includes government assigned identifiers to include passport, alien ID, tax ID, drivers' licenses, etc., of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings and visa applications.
Mother's maiden name	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop includes other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Vehicle identifiers	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop includes vehicle identifiers of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data.</p>
Personal mailing address	X	A, B, C, D	<p>Fusion Desktop includes personal contact information of targets of investigations and their associates as well as members of the public (US and non-USPERs), and names of investigative personnel including case agents and federal attorneys, included through source data.</p> <p>Fusion Desktop workflow also includes a limited subset (email address and phone but NOT physical addresses) for OFC employees (contractor and federal employees) for workflow process and auditing purposes.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Personal e-mail address	X	A, B, C, D	<p>Fusion Desktop includes personal contact information of targets of investigations and their associates as well as members of the public (US and non-USPERs), and names of investigative personnel including case agents and federal attorneys, included through source data.</p> <p>Fusion Desktop workflow also includes a limited subset (email address and phone but NOT physical addresses) for OFC employees (contractor and federal employees) for workflow process and auditing purposes.</p>
Personal phone number	X	A, B, C, D	<p>Fusion Desktop includes personal contact information of targets of investigations and their associates as well as members of the public (US and non-USPERs), and names of investigative personnel including case agents and federal attorneys, included through source data.</p> <p>Fusion Desktop workflow also includes a limited subset (email address and phone but NOT physical addresses) for OFC employees (contractor and federal employees) for workflow process and auditing purposes.</p>
Medical records number			<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Health information or records are currently not included in Fusion Desktop unless otherwise reported as part of law enforcement case reporting narratives.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Medical notes or other medical or health information			<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Health information or records are currently not included in Fusion Desktop unless otherwise reported as part of law enforcement case reporting narratives.</p>
Financial account information	X	C, D	<p>** Data is used solely for software development and testing of the Fusion Desktop application on Oak Island. **</p> <p>Fusion Desktop includes financial information of the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Applicant information			
Education records	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Military status or other information	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Employment status, history, or similar information	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes other personal information on the targets of investigations and their associates as well as members of the public (US and non-USPERs) through investigative case report holdings and non-investigative data such as BSA holdings.</p>
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	<p>Fusion Desktop may include employment performance information only on subjects of criminal investigations relevant to OCDETF's mission, from limited data sets such as agency Office of the Inspector General investigative reports.</p>
Certificates			
Legal documents	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop may include legal documents only on subjects of criminal investigations relevant to OCDETF's mission.</p>
Device identifiers, e.g., mobile devices	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes electronic device identifiers of investigation targets and their associates as well as members of the public (US and non-USPERs), and names of investigative personnel including case agents and federal attorneys, included through source data.</p> <p>Fusion Desktop workflow also includes a limited subset (mobile phone) for OFC employees (contractor and federal employees) for workflow process and auditing purposes.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Web uniform resource locator(s)	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes web uniform resource locators of investigation targets and their associates as well as members of the public (US and non-USPERs).</p>
Foreign activities	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes information on foreign law enforcement activity and/or immigrant visas, as the information pertains to criminal investigations and is relevant to OCDETF's mission.</p>
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop and MIS include criminal records through its agency law enforcement investigative case reports. It also includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Juvenile criminal records information	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes criminal records through its agency law enforcement investigative case reports. It also includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop may include information regarding whistleblowers when relevant to OCDETF's mission, gathered from limited data sets such as agency Office of the Inspector General investigative reports.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Grand jury information	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes limited grand jury information under rule 6(e). Such data is strictly access-controlled and limited to investigative personnel and necessary support staff identified by name on relevant 6(e) letters.</p> <p>Fusion Desktop includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes potential witness information as included in agency law enforcement investigative case reports. Fusion Desktop also includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>
Procurement/contracting records			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Proprietary or business information	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop source data, as well as OFC Products and their requests, may contain business contact information.</p> <p>OFC Requests and completed OFC Products contain business contact information for federal employee and other federal government personnel who requested the OFC Products or received disseminated OFC Products,</p>
Location information, including continuous or intermittent location tracking capabilities	X	C, D	<p>** This data MAY be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes location information through its agency law enforcement investigative case reports. It also includes information on criminal prosecution, civil litigation, and administrative proceedings on the targets of active law enforcement investigations, including case reporting from the OCDETF MIS case management system and other federal case management systems.</p>
Biometric data:			
- Photographs or photographic identifiers	X	A, B, C, D	<p>** This data MAY temporarily be stored on Oak Island servers solely for the purpose of software development and testing**</p> <p>Fusion Desktop includes limited photos as part of investigative case files and visa applications. Fusion Desktop does not hold videos, voice recordings, or other biometrics.</p> <p>Fusion Desktop's "roster" displays photos of OFC employees along with their official contact information. These photos are not fused with or otherwise combined with Fusion Desktop investigative information.</p>

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- Video containing biometric data			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Fingerprints			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Palm prints			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Iris image			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Dental profile			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Voice recording/signatures			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Scars, marks, tattoos			Fusion Desktop includes criminal records through its agency law enforcement investigative case reports, which may contain this data.
- Vascular scan, e.g., palm or finger vein biometric data			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- DNA profiles			Fusion Desktop does not hold videos, voice recordings, or other biometrics.
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.
- User passwords/codes	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.
- IP address	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.
- Date/time of access	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detainees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
- Queries run	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.
- Contents of files	X	A, B	Fusion Desktop maintains relevant auditing and administrative data pursuant to federal information system requirements, to include attributable user IDs, IP addresses, date/time of access, etc.
Other (please list the type of info and describe as completely as possible):			

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers	X				
Other (specify): Informants and Interested Third Parties					

Section 4: Information Sharing

4.1 *Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.*

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
Within the Component	X		X	Access to DOJ information systems must be granted prior to granting access to Oak Island. OFC Fusion Desktop and MIS information can only be accessed through a unique login to the system, given only upon application by users. Allows OCDETF and partners to develop investigative leads, operational intelligence products, and strategic intelligence assessments on new or evolving threats for dissemination as appropriate to cognizant law enforcement, regulatory, intelligence, and military agencies to assist them in enforcing criminal, civil, and regulatory laws related to organized crime

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
DOJ Components	X		X	Access to Oak Island is limited to detailees to the OCDETF Fusion Center, whose unique login access request is reviewed and approved prior to granting an Oak Island account; all access goes through DOJ intranet enabled workstation. Allows OCDETF and partners to develop investigative leads, operational intelligence products, and strategic intelligence assessments on new or evolving threats for dissemination as appropriate to cognizant law enforcement, regulatory, intelligence, and military agencies to assist them in enforcing criminal, civil, and regulatory laws related to organized crime
Federal entities	X			Access to Oak Island is limited to detailees to the OCDETF Fusion Center, whose unique login access request is reviewed and approved prior to granting an Oak Island account; all access goes through DOJ intranet enabled workstation. Allows OCDETF and partners to develop investigative leads, operational intelligence products, and strategic intelligence assessments on new or evolving threats for dissemination as appropriate to cognizant law enforcement, regulatory, intelligence, and military agencies to assist them in enforcing criminal, civil, and regulatory laws related to organized crime
State, local, tribal gov't entities				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct log-in access	Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.
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				None
Foreign entities				None
Other (specify):				

- 4.2 *If the information will be released to the public for “[Open Data](#)” purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the federal government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.*

N/A

Section 5: Notice, Consent, Access, and Amendment

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

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. See 28 C.F.R. § 16.135.

Notice is also provided by the Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System, JUSTICE/OCDETF-002, 78 Fed. Reg. 56926 (Sept. 16, 2013) (updated 82 Fed. Reg. 24151, 160 (May 25, 2017), available at <https://www.gpo.gov/fdsys/pkg/FR-2013-09-16/pdf/2013-22368.pdf>, and the Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS) System of Records Notice, JUSTICE/OCDETF-001, 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), available at <https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf>.

5.2 *What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.*

Investigative information is not gathered directly from individuals but from contributing agency records (and notice is not generally provided by the contributing agencies, and consent not requested, for the reasons in 5.1 and 5.3). Contributing agencies include contact information for law enforcement personnel and prosecutors assigned to each case. This information is voluntarily submitted to the OFC and/or MIS by these individuals as part of the standard operating procedure for OCDETF cases. 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 MOU with OCDETF.

5.3 *What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.*

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

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

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

Section 6: Maintenance of Privacy and Security Controls

6.1 *The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).*

X	<p>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):</p> <ul style="list-style-type: none"> • DOJ OCIO infrastructure which houses Fusion Desktop: ATO valid 5/8/2024 – 5/7/2027 • Oak Island: ATO valid 4/14/2023 – 4/13/2026 • MIS: ATO valid 9/23/2022 – 9/23/2025
---	--

	<p>If an ATO has not been completed, but is underway, provide status or expected completion date: N/A</p> <p>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:</p> <p>Oak Island has two (2) open POA&Ms as of December 2024, the details of which are available within the DOJ JCAM database:</p> <ul style="list-style-type: none"> • POA&M #43962: Forward all applicable event/audit logs to the DOJ Enterprise logging system. POA&M currently delayed due to awaiting resources both on OCDETF IT services contract and at DOJ CSS to configure additional event log indices and verify. • POA&M #73682: Upgrade Oak Island Linux server software versions.
	<p>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:</p>
X	<p>This system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with FIPS 199. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan:</p> <p>Oak Island is FIPS 199 categorized Moderate Confidentiality, Moderate Integrity, and Low Availability, with an overall categorization of Moderate. The factors for these determinations include:</p> <ul style="list-style-type: none"> • Moderate Confidentiality: Data in Oak Island, particularly as used to develop and test other OCDETF systems such as Fusion Desktop, may include information on open, active law enforcement investigations, the unauthorized disclosure of which could cause serious adverse impact on those investigations. • Moderate Integrity: Completed OFC work products incorporate information from the data sources housed in the Fusion Desktop and data accessed from Oak Island. Unauthorized modification or destruction of this information would have serious adverse impact on the integrity of OFC work products and the law enforcement missions that these work products support, through incorrect or omitted information on targets of those law enforcement investigations. • Low Availability: Outages of the Oak Island system and its components could cause limited adverse effects on the operations of both the OFC and the broader OCDETF mission.
X	<p>Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:</p> <p>The security and privacy controls listed in the MIS, Oak Island, and Fusion Desktop 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.</p>

	This is part of a continuing monitoring program that is in place within the MIS, Oak Island, and Fusion Desktop operating environment. Oak Island security and privacy controls are assessed annually or as required more often based on system changes and updates. The vulnerability scans are performed continuously via a combination of tools per Department policies, with daily reporting to the DOJ enterprise cybersecurity portal.
X	<p>Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:</p> <p>Auditing is in place within the Oak Island operating environment and methods to consistently improve procedures are in place. Audit logs are reviewed as required by DOJ on a weekly basis. Oak Island audits all end user and system activities in accordance with OMB M-21-31 requirements, including but not limited to:</p> <ul style="list-style-type: none"> • Date/timestamps of audited activity • User or system process conducting the activity, including source and destination network information <p>OCDETF also generates periodic audit reports made available to contributing data providers on the use of their data, including the information described above.</p> <p>Auditing is in place within the MIS and Oak Island operating environments, and methods to consistently improve procedures are in place. Audit logs are reviewed as required by DOJ on a weekly basis. Audit logs are maintained for searching of defendants and prospective defendants. The ISSO and monitoring admins are responsible for review.</p>
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	<p>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:</p> <p>DOJ required Privacy Training is completed by all required system individuals.</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?

OCDETF complies with Department and Federal policies and requirements on security and privacy of all information within the Oak Island system. Data at rest (DAR) is encrypted using approved FIPS 140-2³ algorithms, including Advanced Encryption Standard (AES-256). OCDETF is in the process of reviewing requirements for DAR encryption to comply with post-

³ FIPS 140-2 specifies the security requirements for encrypting information and is available at: <https://csrc.nist.gov/pubs/fips/140-2/upd2/final>.

quantum computing requirements, expected to be completed by 2027. Data in transit is protected using TLS 1.2 and greater (Transport Layer Security).

Oak Island is expected to meet all applicable FISMA access (AC) and auditing (AU) controls appropriate for a FIPS 199 Moderate categorized system. OCDETF regularly audits all Oak Island system access and usage (as described above) for inappropriate access, usage, and disclosure of information, and has an Incident Response Plan in place for the Oak Island system to coordinate any incident responses with the DOJ Security Operations Center (JSOC) per Department policy.

Oak Island is located in a secure facility on the secure DOJ Intranet network. 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. 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 Oak Island, 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.

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.)*

Currently, OCDETF OFC products are "Permanent" because they are Unscheduled. OCDETF is working with the DOJ Justice Management Division to create a new records schedule to submit for approval by NARA.

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 users will sign the OCDETF Rules of Behavior for each account. Policy documents that govern the protection of the data are U.S. Department of Justice DOJ Order 0904 Cybersecurity Program, and applicable System Security and Privacy Plan (SSPP) with 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.

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-002

System Name: Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System

Federal Register: 78 Fed. Reg. 56926 (Sept. 16, 2013) (updated 82 Fed. Reg. 24151, 160 (May 25, 2017), available at <https://www.gpo.gov/fdsys/pkg/FR-2013-09-16/pdf/2013-22368.pdf>

System Number: JUSTICE/OCDETF-001

System Name: Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS)

Federal Register: 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), available at <https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf>.

Section 8: Privacy Risks and Mitigation

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

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.*

OCDETF Oak Island implements security and privacy safeguards and controls that are both

administrative and physical to reduce the risk to compromise PII information.

Administratively, access to information within this network 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 Oak Island system. The only people who qualify for such access are a small number of OCDETF technical employees with appropriate background investigations. These technical employees can only use this access in a DOJ controlled facility and hosted platform.

All users with access to the systems are U.S. citizens with appropriately adjudicated background investigations and hold a Secret security clearance or higher. Access to OCDETF Oak Island, MIS, and Fusion Desktop systems is restricted to authorized employees, system administrators, and security and operations staff. Access to Fusion Desktop is further limited to DOJ OCIO network infrastructure from the OCDETF Fusion Center location excepting contingency operations following activation of the approved information systems contingency plan (ISCP), under which Fusion Desktop may be accessible from DOJ OCIO network infrastructure at alternate locations. All users are required to agree to the rules of behavior for OCDETF system access, must take cyber security awareness training within their agencies, and receive specific OFC training throughout the year from OCDETF.

A second layer of protection is provided by virtue of the designs and implementations of the OFC Fusion Desktop, Oak Island, and MIS. Moreover, users are made aware of the ramifications of revealing OCDETF information to unauthorized individuals through the rules of behavior, which they must agree. Penalties for such behaviors range from suspensions to firings to prison sentences.

Mitigation of Misuse by Authorized Individuals: OCDETF determines user access of information for all OCDETF 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 language is included on the OFC Employee Security Agreement and must be certified by the requester when gaining access to the OFC and its systems:

“By signing, I am verifying that I will adhere to all security procedures, and that I understand the sensitivity and importance of safeguarding and handling NSI. I am aware that any questions I have concerning Security here at the Merrifield Facility should be directed to my Manager and/or my servicing Security Officer. Your compliance in taking the above measures will help ensure that we are operating in accordance with the rules set by DOJ Security and Emergency Planning Staff and will safeguard NSI, DEA, and Law Enforcement Sensitive material.”

Audit logs are maintained to capture certain actions, queries, and search terms, within the OCDETF systems. 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 Oak Island access request processes were 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 persons who are authorized for OCDETF system accounts must be appropriately cleared for such access by the users' home agency and by OCDETF Security prior to obtaining OCDETF system 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 OFC and MIS. User access to the OCDETF OFC 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 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 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 system(s) access.

Additionally, Oak Island requires public key infrastructure (PKI)⁴ cards to access, and all passwords expire after 60 days. Upon password expiration, a system administrator must be contacted to renew the password. Prior to renewing any password after expiration, the OCDETF system administrator is required to contact the password user's specific agency to confirm the propriety of such user's access renewal. If the user's account is deactivated, the user is required to re-apply for access to the system. Users can also renew their passwords prior to the 60-day expiration. However, all accounts are reviewed annually regardless of password expiration. All users are required to read and acknowledge understanding of the Rules of Behavior before using OCDETF IT resources.

General notice of the system of records is provided to the public in the following OCDETF SORNs: the Organized Crime Drug Enforcement Task Force Fusion Center and International Organized Crime Intelligence and Operations Center System, JUSTICE/OCDETF-002, 78 Fed. Reg. 56926 (Sept. 16, 2013) (updated 82 Fed. Reg. 24151, 160 (May 25, 2017), *available at*

⁴ PKI provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and the storage of sensitive verification system data within identity cards and the verification system. See https://csrc.nist.gov/glossary/term/public_key_infrastructure.

<https://www.gpo.gov/fdsys/pkg/FR-2013-09-16/pdf/2013-22368.pdf>, and the Organized Crime Drug Enforcement Task Forces Management Information System (OCDETF MIS) System of Records Notice, JUSTICE/OCDETF-001, 78 Fed. Reg. 56737 (Sept. 13, 2013), updated 82 Fed. Reg. 24151, 160 (May 25, 2017), *available at* <https://www.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf>.