Executive Office for the

Organized Crime Drug Enforcement Task Forces

Privacy Impact Assessment
for the
OCDETF Fusion Desktop Application

Issued by:

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

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

Date approved: November 11, 2023

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 OFC Fusion Desktop application (Fusion Desktop) is an application that constitutes the single largest repository of federal and foreign investigative reporting throughout the federal government. Since the OFC combines casework and intelligence from across member agencies to conduct data integration and analysis, the Fusion Desktop is the tool that allows information from all federal partners to illuminate criminal networks and allow investigators and prosecutors to effectively coordinate investigative and prosecutorial efforts for their greatest effect.

All information maintained in the OFC Fusion Desktop is contributed by OCDETF's federal member agencies: the Department of Justice (DOJ) Drug Enforcement Administration (DEA), the Federal Bureau of Investigation, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the United States Marshals Service; Criminal Division; Executive Office for U.S. Attorneys; the Department of the Treasury's Criminal Investigation Division of the Internal Revenue Service; the Department of Homeland Security's Immigration and Customs Enforcement, Customs and Border Protection, and U.S. Coast Guard; the Department of Labor and Office of the Inspector General; the United States Postal Service and Postal Inspection Service; the United States Secret Service; the Department of State Diplomatic Security Service; Environmental Protection Agency; Fish and Wildlife Services; in cooperation with the DOJ's United States Attorney's Offices. This information is entered and uploaded into the OFC Fusion Desktop by trained OFC

personnel with appropriate data entry access. The OFC Fusion Desktop is a web[1] application that provides storage and retrieval of such investigation and prosecution information for use by OFC 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 OFC Fusion Desktop provides a paperless and simplified environment for data entry and reporting; provides OCDETF and its partner agencies with 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.

The information flow on the Fusion Desktop is described at a high level as follows: Approved personnel at member agencies (all member agencies are federal agencies, including both DOJ and non-DOJ agencies) send information requests to OCDETF through a data ingest pipeline. In response to those member agency requests, OCDETF personnel (only OCDETF employees, contractors, and OCDETF-controlled detailees and task force officers) located within OCDETF-controlled space at the DOJ then access the OCDETF Compass database to run searches, analyze data, and compile reports to return to the requesting agencies. Upon case coordination review, classification review, and approval for dissemination, OCDETF personnel then disseminate those reports through the same portal, back to the member agency requesters, which the requesters receive via the same OCDETF Web Portal.

This Privacy Impact Assessment was conducted by OCDETF to ensure the highest level of compliance with relevant privacy and information laws and regulations, determine the privacy risks associated with this information system, and evaluate ways to reduce any privacy risks.

Section 2: Purpose and Use of the Information Technology

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

The OFC conducts cross-agency integration and analysis of its data holdings to create comprehensive, fused intelligence pictures of targeted organizations, including those identified as Consolidated Priority Organization Targets (CPOTs) and Regional Priority Organization Targets (RPOTs). The OFC passes actionable leads directly to OCDETF participants in the field as well as through the DEA-led, multi-agency Special Operations Division (SOD), including the OCDETF Co-Located Strike Forces. These leads ultimately result in the development of better-coordinated, more comprehensive, multi-jurisdictional OCDETF investigations of the most significant drug trafficking and money laundering networks. Additionally, the OFC creates

[1] This data repository is hosted in a non-cloud DOJ data center on a classified network.

strategic intelligence products for enhanced threat analysis which support national strategic efforts against transnational organized crime (TOC).

The OFC Fusion Desktop application is the central information system used by staff at the OFC to complete their mission. Fusion Desktop provides users a unified analytic platform for request and product workflow and fused data searching. Fusion Desktop's Compass search engine fuses data from disparate data sources and identifies previously unidentified relationships between elements of those data sources.

Using this system, the OCDETF OFC and OCDETF's International Organized Crime Intelligence and Operations Center (IOC-2) 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 drug trafficking, money laundering, firearms trafficking, alien smuggling, organized crime, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States' national and international security interests through their involvement in such crimes.

Fusion Desktop is made up of four subcomponents: the data ingest pipeline, the Compass database, the Compass search engine, and the OFC Product workflow.

- The data ingest pipeline performs Extraction, Translation, and Loading (ETL) functions to load source data from OCDETF member agencies and partners into the Compass database as searchable persistent information available to the Fusion Desktop. Data providers retain ownership of the information provided to the OFC, and Memoranda of Understanding (MOUs) with each member agency govern the specific data provided and the terms of its usage at the OFC.
- The Compass database stores data which has been processed through the ETL pipeline and prepared for search. All data is encrypted both at rest and in transit between the data and application servers, using FIPS 140-2 validated cryptographic algorithms.
- The Compass search subcomponent provides "free text" and "fuzzy" search capabilities across the OFC's data warehouse. OFC analysts use Compass to rapidly search and analyze ingested source documents and structured data from various government agency data sources.
- The OFC Product workflow subcomponent provides end-to-end request and product workflow for Fusion Center investigative product requests, culminating in completed investigative briefs known as OFC Products. When completed (including review and approval by agency representatives for any agency whose data is included in the OFC Product), OFC Products are disseminated to requesters and to related personnel such as involved federal case agents and federal prosecutors. Requests for products are made via the OCDETF Web Portal, available on OFC member and partner agency intranet websites, and completed OFC Products delivered for pickup via the same OCDETF Web Portal.

The Fusion Desktop provides system development, management, maintenance, and mission support infrastructure for OCDETF and OCDETF OFC. 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).

The Fusion Desktop's data warehouse is made up of that investigative case information, 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 and/or 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, the Fusion Desktop maintains PII on its end users (for auditing and workflow purposes) to include name, official email, and phone numbers, as well as OFC Product requesters and recipients.

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
- Email Addresses
- Personal Names
- Home Addresses
- Business Addresses
- IP Addresses
- Law Enforcement Identification Numbers
- Social Media IDs/Monikers
- Passport Numbers
- Driver's License Numbers

Fusion Desktop Users

Only OCDETF personnel are users or have access to the system. Such personnel include OCDETF employees, OCDETF task force officers,[2] and OCDETF contractors, all of whom can perform searches and view documents from search results. Only approved IT administration personnel have elevated access to write or delete from the system. All users with access to the Fusion Desktop are U.S. citizens with appropriately adjudicated background investigations and hold a Secret security clearance or higher.

Access to the Fusion Desktop is restricted to authorized employees, task force officers, system administrators, and security and operations staff. Access is limited users at 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 alternate locations. The bulk of information in Fusion Desktop is law enforcement sensitive, but some documents may be classified at the SECRET level.

Completed OFC Products are disseminated to OCDETF member agency federal government and contractor personnel for attributed, audited download via an OCDETF Web Portal, with access limited to participating agency sensitive-but-unclassified intranets. The OCDETF Web portal requires a login, which is approved for specific OCDETF member agency personnel by OFC.

The Fusion Desktop is a new information system which is undergoing the ATT/ATO accreditation process. The Fusion Desktop is based on the current, accredited Fusion system hosted on DEA network infrastructure and represents the to-be state of an ongoing IT migration project to move hosting off DEA networks and onto DOJ OCIO network infrastructure.

OCDETF contractors serve as both the system administrators as well as a significant component of Fusion Desktop end users. OCDETF employee supervisors must approve disclosure of information as part of the Fusion Desktop operations.

End users use, process, and disseminate information from the Fusion Desktop application. Use includes OCDETF contractors performing searches of OFC information (Compass search) and compiling completed OFC Products which may incorporate OFC information.

OCDETF contractors may store and maintain information on the Fusion Desktop system as part of normal system operations. Where required, contractors may dispose of information as part of operating Fusion Desktop pursuant to relevant retention and disposition policies.

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

---

[2] Task force officers are non-DOJ employees or contractors who are on detail to and under the direction of OCDETF for purposes of the task force.

Authority	Citation/Reference
Statute	- Title 21 U.S.C § 878, Controlled Substance Act - Title 18 U.S.C § 2518, (1) (e), Crimes and Criminal Procedures - Consolidated Appropriations Act, 2004, Public Law 108–199, 118 Stat. 3 - Comprehensive Drug Abuse Prevention and Control Act of 1970, Public Law 91– 513, 84 Stat. 1236 (21 U.S.C. § 801 *et seq.*) - Organized Crime Control Act of 1970, Public Law 91–452, 84 Stat. 922
Executive Order	- Executive Order 11396, 33 Fed. Reg. 2689 (1968), 3 C.F.R. 1966-1970 Comp. p. 711. - Executive Order 13773, 82 Fed. Reg. 10691 (2017), pp. 10691-10693.
Federal regulation	*See id.*
Agreement, memorandum of understanding, or other documented arrangement	- United Nations Single Convention on Narcotic Drugs, 1961 - United Nations Convention on Transnational Organized Crime, 2000
Other (summarize and provide copy of relevant portion)	Strategy to Combat Transnational Organized Crime, July 2011, *available* here.

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Name:	X	A, B, C, D	Fusion Desktop includes 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. Fusion Desktop workflow also includes the same info as above (via OFC Products and requests for the same), along with OFC employees (contractor and federal employees) for workflow process and auditing purposes.
Date of birth or age	X	C, D	Fusion Desktop includes dates of birth or ages 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.
Place of birth	X	C, D	Fusion Desktop includes places of birth 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.
Gender	X	C, D	Fusion Desktop includes the gender 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.
Race, ethnicity, or citizenship	X	C, D	Fusion Desktop includes race or ethnicity 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.

(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
Religion	X	C, D	Fusion Desktop includes the religion 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.
Social Security Number (full, last 4 digits or otherwise truncated)	X	C, D	Fusion Desktop 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.
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 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
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	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.
Vehicle identifiers	X	C, D	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.
Personal mailing address	X	A, B, C, D	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. 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.
Personal e-mail address	X	A, B, C, D	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.

(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
Personal phone number	X	A, B, C, D	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.
Medical records number	X	A, B, C, D	Health information or records are currently not included in Fusion Desktop unless otherwise reported as part of law enforcement case reporting narratives.
Medical notes or other medical or health information	X	A, B, C, D	Health information or records are currently not included in Fusion Desktop unless otherwise reported as part of law enforcement case reporting narratives.
Financial account information	X	C, D	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.
Applicant information			
Education records	X	C, D	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.
Military status or other information	X	C, D	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.
Employment status, history, or similar information	X	C, D	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.

(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
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	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.
Certificates			
Legal documents	X	A, B, C, D	Fusion Desktop may include legal documents only on subjects of criminal investigations relevant to OCDETF's mission.
Device identifiers, e.g., mobile devices	X	A, B, C, D	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. Fusion Desktop workflow also includes a limited subset (mobile phone) for OFC employees (contractor and federal employees) for workflow process and auditing purposes.
Web uniform resource locator(s)	X	C, D	Fusion Desktop includes web uniform resource locators of investigation targets and their associates as well as members of the public (US and non-USPERs).
Foreign activities	X	A, B, C, D	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.
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	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.

(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
Juvenile criminal records information	X	A, B, C, D	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.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	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.
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, D	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.
Grand jury information	X	A, B, C, D	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. 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.

(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
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	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.
Procurement/contracting records			
Proprietary or business information	X	A, B, C, D	Fusion Desktop source data, as well as OFC Products and their requests, may contain business contact information. 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,
Location information, including continuous or intermittent location tracking capabilities	X	C, D	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.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	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. 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.

(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
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **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**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **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.
- **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.

(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
- **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): Foreign partner data may be included in information provided by federal partner agencies.					

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 Intranet enabled workstation must be granted prior to granting access to the OCDETF Fusion Desktop, and/or specific OFC Fusion Desktop product must be shared with authorized user through the OCDETF Web Portal Account. 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 DOJ Intranet enabled workstation must be granted prior to granting access to the OCDETF Fusion Desktop, and/or specific OFC Fusion Desktop product must be shared with authorized user through the OCDETF Web Portal Account. 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			Shared via the OCDETF Web Portal, which is accessible only to OFC-authorized accounts from OCDETF member agencies' authorized federal law enforcement intranets. Allows OCDETF to develop investigative leads, operational intelligence products, and strategic intelligence assessments on new or evolving threats for dissemination as appropriate to OCDETF member agencies to assist them in enforcing laws related to organized crime.
State, local, tribal gov't entities				
Public				

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments	X			Restricted Access to investigative documentation for law enforcement through mutual legal assistance treaty (MLAT) process. No direct access.
Foreign entities				
Other (specify):				

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

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.

Notice is 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.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 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 certain notice, access and amendment provisions of the Privacy Act. Making this information subject to such requirements risks circumvention of the law. *See* 28 C.F.R. § 16.135.

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

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

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The Fusion Desktop Application is not yet fully operational and is expected to receive its ATO in November 2023 and be fully operational by January 2024, at which time the existing FUSION system will be retired. The Fusion Desktop Application will replace the FUSION system. Fusion Desktop operates on secure network infrastructure, which has an active ATO valid from 5/18/2021 – 5/17/2024.

	If an ATO has not been completed, but is underway, provide status or expected completion date: ATO expected completion date is approximately November 2023. Fusion Desktop is operating under an Authorization to Test (ATT) granted in April 2023 and continues to assess security and privacy controls for the full ATO. **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:** As of August 2023, and based on control assessments to date, OCDETF does not anticipate opening any security or privacy POA&Ms in conjunction with the FUSION DESKTOP ATO.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**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:** Fusion Desktop is FIPS 199 categorized High Confidentiality, High Integrity, and High Availability, with an overall categorization of High. The factors for these determinations include: • High Confidentiality: Data in Fusion Desktop includes information on open, active law enforcement investigations, the unauthorized disclosure of which could cause severe or catastrophic impact on those investigations. • High Integrity: Completed OFC work products incorporate information from the data sources housed in the Fusion Desktop. Unauthorized modification or destruction of this information would have severe or catastrophic 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. • High Availability: Outages of the Fusion Desktop system and its components would cause severe or catastrophic adverse effects on the operations of both the OFC, and on the broader OCDETF mission. Fusion Desktop system components are in use 24x7, either by end users, automated data processes, or system administration activities.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The security and privacy controls listed in the 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. This is part of a continuing monitoring program that is in place within the Fusion Desktop operating environment. The OCDETF Fusion Desktop maintains PII for prospective defendants, defendants, case attorneys, case agents, and OCDETF Fusion Desktop users. Fusion Desktop 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	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Auditing is in place within the Fusion Desktop operating environment and methods to consistently improve procedures are in place. Audit logs are reviewed as required by DOJ on a weekly basis. Fusion Desktop audits all end user and system activities in accordance with OMB M-21-31 requirements, including but not limited to: • Date/timestamps of audited activity • User or system process conducting the activity, including source and destination network information • All search terms and parameters used to search data stored in Fusion Desktop • All results returned as a result of a search of the data stored in Fusion Desktop • All views of any data stored in Fusion Desktop • All review and approval/disapproval for dissemination of data outside of the OFC, including the intended recipient(s) and whether (and when) those recipients received OFC products OCDETF also generates periodic audit reports made available to contributing data providers on the use of their data, including the information described above.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** DOJ required Privacy Training is required of and completed by all system users. Although not privacy-specific, all users \are required to undergo a comprehensive training with an experienced OCDETF Fusion Desktop trainer to ensure proper handling of information and data integrity.

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 Fusion Desktop system. Data at rest (DAR) is encrypted using approved (Federal Information Processing Standards (FIPS) 140-2[3] algorithms, including

[3] FIPS 140-2 specifies the security requirements for encrypting information and is available at:

Advanced Encryption Standard (AES-256)[4]. OCDETF is in the process of reviewing requirements for DAR encryption to comply with post-quantum computing requirements, expected to be completed by 2027. Data in transit is protected using TLS 1.3 (Transport Layer Security)[5].

Fusion Desktop is expected to meet all applicable FISMA access (AC) and auditing (AU) controls appropriate for a FIPS 199[6] High categorized system. OCDETF regularly audits all Fusion Desktop 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 Fusion Desktop system to coordinate any incident responses with the DOJ Security Operations Center (JSOC) per Department policy.

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.

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 approved secure infrastructure. 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 2640.2F, and applicable System Security and Privacy Plan (SSPP) with Approval to Operate (ATO). Recognizing that access to priority target information should be limited for security and privacy reasons, the system was designed to limit access.

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

---

https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

[4] AES-256 is a U.S. Government-approved cryptographic algorithm that can be used to protect electronic data. *See* https://csrc.nist.gov/glossary/term/advanced_encryption_standard.

[5] TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet. *See* https://csrc.nist.gov/glossary/term/transport_layer_security.

[6] FIPS 199 provides a standard for categorizing federal information and information systems according to an agency's level of concern for confidentiality, integrity, and availability and the potential impact on agency assets and operations should their information and information systems be compromised through unauthorized access, use, disclosure, disruption, modification, or destruction. https://csrc.nist.gov/pubs/fips/199/final.

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).

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.***

As described above in Section 2, Fusion Desktop application users are task force members, and all OFC Fusion Desktop data is collected from the OFC member agencies stated in Section 1 for use in developing and enforcing criminal, civil, and regulatory laws related to drug trafficking, money laundering, firearms trafficking, alien smuggling, organized crime, terrorism, and other crimes, including the identification, apprehension, and prosecution of individuals who threaten the United States' national and international security interests through their involvement in such crimes. The data contributed by OCDETF member agencies is collected in accordance to the agencies' own policies and procedures, including procedures for their sources of information; Fusion Desktop application users query those agencies' data for relevant content when creating OFC products about targeted criminal organizations. Only relevant and necessary content is included in reports created and disseminated by OCDETF using the Fusion Desktop.

The OCDETF OFC Fusion Desktop implements security and privacy safeguards and controls that are both administrative and physical in order to reduce the risk to compromise PII information.

Administratively, access to information within these applications are need-to-know only. Role-based access controls are enforced to restrict access and privileged access is assigned to only few system administrators. Only a small number of personnel have direct access to all data in the OCDETF OFC Fusion Desktop 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 OCDETF controlled facility and hosted platform.

Fusion Desktop is only accessible to the following personnel, all of whom can only exercise such access from OCDETF-controlled space via secure infrastructure: OCDETF employees, OCDETF contractors, OCDETF task force officers, and detailees to OCDETF with need to know. All such persons with direct access to the Fusion Desktop are U.S. citizens with appropriately adjudicated background investigations and hold a Secret security clearance or higher. Access to Fusion Desktop is limited to secure 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 secure infrastructure alternate locations. All users are required to agree to the rules of behavior for OCDETF Fusion Desktop access, must take cyber security awareness training within their agencies, and receive specific OFC training throughout the year from OCDETF.

Only Fusion Desktop application users have direct access to Compass and the OFC applications. Appropriate personnel from OCDETF member agencies (who have an active role in transnational organized crime investigations but are not detailed to the physical OFC) may request information or a product from the OFC by submitting a request through an employee's individual OCDETF Web Portal account, as accessed from participating agency intranets; these requesters do not have direct access to the Fusion Desktop applications. Such member agency personnel users seeking to share OCDETF information with third parties must first clear the request through the OCDETF Fusion Center Director. 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.

A second layer of protection is provided by virtue of the design and implementation of the OFC Fusion Desktop. Moreover, OFC Fusion Desktop users are made aware of the ramifications of revealing OFC information to unauthorized individuals through the rules of behavior, to which they must agree. Penalties for violations 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 OFC Fusion Desktop. 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.

Mitigation of Misuse by Authorized Individuals: OCDETF determines user access of information for all OCDETF OFC Fusion Desktop 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 user 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 Fusion Desktop. OCDETF reviews audit logs on at least a weekly basis, performing manual reviews for suspicious activity and forwarding to DOJ enterprise audit logging services for automated review. 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 Fusion Desktop 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, all users also 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 OFC Fusion Center accounts must be appropriately cleared for such access by the users' home agency and by OCDETF Security prior to obtaining Fusion Desktop 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. 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 OFC Fusion Desktop 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 Fusion Center 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 OFC access.

Additionally, all passwords expire after 60 days. Upon password expiration, a system administrator must be contacted in order to renew the password. Prior to renewing any password after expiration, the OCDETF Fusion Desktop 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 SORN: 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.govinfo.gov/content/pkg/FR-2017-05-25/pdf/2017-10781.pdf.