Drug Enforcement Administration

Privacy Impact Assessment
for the
Ontic Case Management System

Issued by:
James Robert Bryden
DEA Senior Component Official for Privacy

Approved by: Michelle Ramsden
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 5, 2025

(July 2023 DOJ PIA Template)

Section 1: Executive Summary

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

Ontic is a case management system used by the Inspections Division, Insider Threat Section (IST) and Executive Protection Section, Protective Intelligence Unit (ISE) for protection of the DEA workforce and Drug Enforcement Administration (DEA) information. Ontic is a web-based, commercial off the shelf (COTS) technology with analytics capabilities hosted within the commercial cloud environment for government (gov-cloud). Ontic uses analytics to evaluate and identify risk from "trusted DEA insiders" (employees, contractors, TFOs) for IST, and from external threats made against DEA personnel and facilities for ISE. Ontic integrates Federal government data from multiple government-internal systems (as detailed in the 2012 White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs) with commercially available information (CAI) presented to DEA analysts for risk assessment and response actions.

The data in Ontic will encompass Personally Identifiable Information (PII), Personal Health Information (PHI), criminal, legal, cyber activity (on U.S. Government-issued devices), online persona or behavior, and more types. The information could belong to DEA and non-DEA employees, U.S. persons and non-U.S. persons, and in the case of the Protective Intelligence Unit, may include information on persons under the age of 18.

IST and ISE may obtain information in Ontic from any United States Government (USG) Agency, other domestic or foreign government entity, or lawfully from a private sector entity information either obtained through legal process or acquired commercially. This will include government data and commercially available information.

DEA's use of Onitc will be a transition to an electronic case management and analytics system for ISE and IST. Ontic is a software company vendor offering the subject case management and analytics software as a service platform. Through this platform, records will be collected, used, processed, stored, maintained, disseminated and disclosed as authorized and appropriate, and disposed of pursuant to the applicable records schedules.

The ISE and IST programs are staffed by only government staff, not contractors. However, the system will draw from underlying agency recordkeeping systems (e.g. security, Human Resources, and other records) which may in their records lifecycle include involvement by Department of Justice (DOJ) contractors.

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.

Ontic is a web based, commercial government-cloud storage, COTS technology that will serve as an electronic case management and analytics system for ISE and IST. As a case management system, Ontic is used by IST to assess internal threats and by ISE to manage protection of the DEA workforce and DEA information. Ontic analytics support the identification and evaluation of risk from trusted DEA insiders (employees, contractors, Task Force Officers (TFO)) for IST, and from external threats made against DEA personnel and facilities for ISE. The analysis is achieved through the integration of USG data from multiple government-internal systems with commercially available datasets used consistently with applicable authorities and Department policy, then presented to DEA analysts for risk assessment and response actions. IST and ISE may access lawfully obtained information from any USG Agency, other domestic or foreign government entity, and from a private sector entity. (More detail on the USG information used is found in the 2012 White House Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs).

ISE:
The purpose of the Ontic platform for ISE is to use analytics to assist in assessing external threats against DEA facilities and DEA personnel on social media and for internal management of cases for executive protection purposes. Once a threat is identified, the analytic portion of Ontic can assist in determining the identity and location of the person making the threat by searching other public-facing social media posts and viewing other public-facing social media accounts the user has created. This information can then be analyzed using other data and investigative tools to create a more complete profile of the threat, for further action or so that the file can be administratively closed as appropriate. Where applicable, the threat can be located, interviewed, and potentially criminally charged for their actions. The case management system records will be maintained securely within a closed ISE instance.

IST:
The purpose of the Ontic platform for IST is to support the identification and evaluation of risk from trusted DEA insiders (employees, contractors, TFOs) in the context of IST's functions and authorities for deterring, detecting, and mitigating insider threats, including the safeguarding of information from exploitation, compromise, or other unauthorized disclosure based on human behavior on DEA IT systems and other risk under insider threat program authorities. The analytics features will be used with sources of federal government data and commercially available data consistently with applicable law and Department policy. This case management system will support IST's inquiries, which can include security, counterintelligence, user audits and monitoring, and other sources of data for evaluation and determination to close an inquiry or to refer it internally as applicable. The case management system records will be maintained securely in a closed IST instance.

Commercially Acquired Information and other data:
Data in the system may include Ontic-specific and other proprietary Commercially Acquired Information (CAI), along with USG data, used consistently with applicable law and DOJ policy:

- State Civil Court Records Research
- Federal Criminal & Civil Research

- Investigative Research
- Adverse Media Research
- Identity Research
- Dark Web
- Risk Events
- Public-facing Social Media Listening
- Crime Data
- Weather
- Public-facing, "Really Simple Syndication" (RSS) Feeds for that access updates to websites
- Global event alerts and activity

Ontic information may be shared between the IST and ISE in situations concerning threat assessments involving an internal or external actor relating to workplace violence, or for other authorized purposes. All users will be internal to DEA, from Security Programs/Executive Protection (ISE) and Insider Threat (IST), with a limited number of additional authorized DEA users relating to oversight and compliance responsibilities.

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	• 21 U.S.C. §801, et seq., The Controlled Substances Act • 44 U.S.C. § 3541 et seq, Federal Information Security Modernization Act (FISMA) • 44 U.S.C. § 3101 (Authority to Make Records of Agency Actions)
Executive Order	• Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and Responsible Sharing and Safeguarding of Classified Information
Federal Regulation	• 28 C.F.R. Part 0, Subpart R, Drug Enforcement Administration organization and functions • 41 C.F.R. § 102-74, Facility Management
Agreement, memorandum of understanding, or other documented arrangement	
Other (summarize and provide copy of relevant portion)	• DOJ Order 0901, Insider Threat • DOJ Order 1701, Security Programs and Responsibilities • DOJ Order 1705, Executive Protection • DOJ Order 2610.2B, Employment Security Order • DEA Inspection Manual 8811, Insider Threat Prevention and Detection Program • DEA Inspection Manual 8461, DEA Executive Protection Program

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C & D	Names could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Date of birth or age	X	A, B, C & D	Date of birth or age could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Place of birth	X	A, B, C &~~,~~ D	Place of birth could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Gender	X	A, B, C & D	Gender could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Race, ethnicity, or citizenship	X	A, B, C & D	Race, ethnicity, or citizenship could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Religion	X	A, B, C & D	Religion could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C & D	Social security number could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).

(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
Tax Identification Number (TIN)	X	A, B, C & D	Tax identification number could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Driver's license	X	A, B, C & D	Driver's license identifiers could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Alien registration number	X	A, B, C & D	Alien registration number could be collected if applicable for DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Passport number	X	A, B, C & D	Passport number could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Mother's maiden name	X	A, B, C & D	Mother's maiden name could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Vehicle identifiers	X	A, B, C & D	Vehicle identifiers could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Personal mailing address	X	A, B, C & D	Personal mailing address could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Personal e-mail address	X	A, B, C & D	Personal e-mail address could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Personal phone number	X	A, B, C & D	Personal phone number could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Medical records number	X	A, B, C & D	Medical records number could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).

(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
Medical notes or other medical or health information	X	A, B, C & D	Medical notes or other medical or health information could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Financial account information	X	A. B. C & D	Financial account information could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Applicant information	X	A & B	Applicant information could be collected on DEA and other federal government personnel.
Education records	X	A, B, C & D	Education records could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Military status or other information	X	A, B, C & D	Military status or other information could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Employment status, history, or similar information	X	A, B, C & D	Employment status, history, or similar information could be collected on DEA and other federal government personnel and may include collection on members of the public (US or non-USPERs).
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A	Employment performance ratings or other performance information could be collected for DEA personnel.
Certificates	X	A, B, C & D	Certificates could be collected for DEA personnel and incidentally for other government personnel and members of the public (US and non-USPERs).
Legal documents	X	A, B, C & D	Criminal records information or civil law enforcement information, e.g., criminal history, arrests, allegations of violation of civil laws such as tax evasion or fraud could be collected for DEA personnel and for other government personnel and members of the public (US and non-USPERs).

(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
Device identifiers, e.g., mobile devices	X	A, B, C & D	Electronic device identifiers could be collected for DEA personnel and for other government personnel and members of the public (US and non-US-PERs
Web uniform resource locator(s)	X	A, B, C & D	Web URLs could be collected for DEA and other government personnel or members of the public (US or non-USPERs).
Foreign activities	X	A, B, C & D	Foreign activities could be collected for DEA and other government personnel or members of the public (US or non-USPERs).
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C & D	Information related to or compiled for criminal records information, e.g. criminal history, arrests, criminal charges could be collected for DEA personnel and incidentally for other government personnel or members of the public (US or non-USPERs).
Juvenile criminal records information	X	A, B, C & D	Juvenile criminal records information could be collected for DEA or other government personnel or members of the public (US and non-USPERs).
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C & D	Information related to or compiled for civil law enforcement could be collected for DEA personnel and incidentally for other government personnel or members of the public (US or non-USPERs).
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, & D	Information related to whistleblower, e.g. tips, complaints, or referrals, could be collected for DEA personnel and incidentally for other government personnel or members of the public (US or non-USPERs).
Grand jury information	X	A, B, C & D	Information related to or compiled for grand jury proceedings could be collected for DEA personnel and incidentally for other government personnel or members of the public (US or non-USPERs).
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C & D	Information concerning witnesses to criminal matters could be collected for DEA or other government personnel or members of the public (US and non-USPERs).

(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
Procurement/contracting records	X	A, B, C & D	Procurement/contracting records could be collected on employees, and other federal government personnel, and may include collection on members of the public (US or non-USPERs).
Proprietary or business information	X	A, B, C & D	Business information could be collected on employees, and other federal government personnel, and may include collection on members of the public (US or non-USPERs).
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C & D	Location information could be collected for DEA or other government personnel or members of the public (US and non-USPERs).
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C & D	Photographs could be collected for DEA personnel and incidentally for other government personnel or members of the public (US or non-USPERs).
- **Video containing biometric data**	X	A, B, C & D	Video could be collected for DEA or other government personnel or members of the public (US and non-USPERs).
- **Fingerprints**	X	A, B, C & D	ISE: To the extent needed to identify a person who commits a crime against a DEA employee or facility
- **Palm prints**	X	A, B, C & D	ISE: To the extent needed to identify a person who commits a crime against a DEA employee or facility
- **Iris image**			
- **Dental profile**	X	A, B, C & D	ISE: To the extent needed to investigate incidents of assault against a DEA employee
- **Voice recording/signatures**	X	A, B, C & D	Voice recording/signatures could be collected for DEA or other government personnel or members of the public (US and non-USPERs).
- **Scars, marks, tattoos**	X	A, B, C & D	Scars, marks, and tattoos could be collected for DEA or other government personnel or members of the public (US and non-USPERs).
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	A, B, C & D	ISE: To the extent needed for investigation of incidents of assault or other crimes or threats against a DEA employee

(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
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A & B	User ID information could be collected for DEA or other government personnel.
- **User passwords/codes**	X	A & B	User passwords/codes could be collected for DEA or other government personnel.
- **IP address**	X	A & B	IP address could be collected for DEA or other government personnel.
- **Date/time of access**	X	A & B	Date/time of access could be collected for DEA or other government personnel.
- **Queries run**	X	A & B	Queries run could be collected for DEA or other government personnel.
- **Contents of files**	X	A & B	Contents of files could be collected for DEA or other government personnel.
Other (please list the type of info and describe as completely as possible):	X	A, B, C & D	Commercially Acquired Information on individuals could be obtained where relevant to an investigation. See Section 2.1

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	X	Hard copy: mail/fax	X	Online	X
Phone	X	Email	X		
Other (specify):					

Section 4: Information Sharing

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

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component	X			IST: To Office of Professional Responsibility (OPR) for referrals; in certain limited circumstances on a need-to-know basis when required if IST must share certain information with other DEA offices in requesting follow up information
DOJ Components	X			ISE: May share information with DOJ components who have been subject to similar threats from the suspect IST: With FBI for any counterintelligence referrals required by 50 U.S.C. § 3381
Federal entities	X			ISE: May share information with other federal entities who have also received similar threats from the suspect. IST: With other Federal entities to the extent authorized by the Privacy Act and routine uses, including for law enforcement purposes
State, local, tribal gov't entities	X			ISE: May share information with other State, Local, and Tribal government entities who have also received similar threats from the suspect IST: With State, Local, and Tribal government entities to the extent authorized by the Privacy Act and routine uses, including for law enforcement purposes
Public	X			In the event of any public incident, for DEA Public Affairs to communicate DEA's activities to the public to a limited extent as

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.**
				appropriate, consistent with applicable SORNs
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			As appropriate, in the form of written records delivered securely such as by JEFS/USAfx or another TC-approved mechanism, and testimony in cooperation with appropriate DOJ counsel (e.g. U.S. Attorney's Offices) or State or Local prosecutors, for criminal justice purposes
Private sector				
Foreign governments	X			As necessary to share information with foreign governments which have also received similar threats from the suspect
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.

Information will not be published on Data.gov, because the information in this system is protected from release under privacy exemptions and criminal investigative data restrictions.

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.

Ontic is not collecting information directly from the individuals who are the subject of investigations. To the extent that individuals carry out public activities for which lawful investigative and protective activity is necessary, DEA has the authority and responsibility to protect its workforce and facilities through case monitoring and follow up as described. Generally, investigative information collected by other systems from which Ontic may have

information transferred from do not include notice as that would undermine the law enforcement purposes of the collection. However, general notice through the publication in the Federal Register of Systems of Records Notices (SORNs) has been provided for the various systems of records used by DEA and DOJ to contain such information.

ISE:

- DOJ-011, *Access Control System*, 69 Fed. Reg. 70279 (Dec. 03, 2004)(full text); 82 Fed. Reg. 24147 (May, 25, 2017)(amendment). https://www.gpo.gov/fdsys/pkg/FR-2004-12-03/pdf/04-26590.pdf
- DOJ-020, *DOJ Identity, Credential, and Access Service Records System,* 84 Fed. Reg. 60110 (Nov. 7, 2019)(full text); https://www.govinfo.gov/content/pkg/FR-2019-11-07/pdf/2019-24246.pdf
- DEA-008, *Investigative Reporting and Filing*, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May, 25, 2017)(amendment). https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf
- DEA-010, *Planning and Inspection Division Record*s, 52 Fed. Reg. 47182, 213 (Dec. 11, 1987)(full text); 66 Fed. Reg. 8425 (Jan. 31, 2001); 82 Fed. Reg. 24147 (May, 25, 2017)(amendments). https://www.justice.gov/opcl/docs/52fr47182.pdf
- DEA-013, *Security Files,* 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)(full text); 66 Fed. Reg. 8425 (Jan. 31, 2001); 82 Fed. Reg. 24147 (May, 25, 2017)(amendments). https://www.justice.gov/opcl/docs/52fr47182.pdf

IST:

- DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (Jul. 14, 2021)(full text). https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf
- DOJ-006, *Personnel Investigation and Security Clearance Record for the Department of Justice*, 67 Fed. Reg. 59864 (Sep. 24, 2002)(full text); *69 Fed. Reg. 65224 (11-10-2004); 82 Fed. Reg. 24147 (May, 25, 2017) (amendments).* https://www.gpo.gov/fdsys/pkg/FR-2002-09-24/pdf/02-24206.pdf
- DOJ-018, *DOJ Insider Threat Program Records,* 82 Fed. Reg. 25812 (Jun. 05, 2017)(full text); 82 Fed. Reg. 27872 (Jun. 19, 2017)(correction). https://www.gpo.gov/fdsys/pkg/FR-2017-06-05/pdf/2017-11445.pdf

In addition, internal DEA workstations and communications equipment contain a warning banner that notifies all DEA systems users at login that any information transmitted through the system may be monitored, intercepted, searched, and/or seized by the Department and that users therefore have no reasonable expectation of privacy in such information.

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.

Due to the law enforcement nature of this system, individuals generally have no role in the collection, use or dissemination of their information in this system. To the extent some

information in Ontic comes from DOJ background investigations, individuals did voluntarily consent to collection or specific uses of some PII.

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.

Because information in this system may be used for law enforcement investigation as well as Security Programs administrative inquiries, access would be allowed to individuals only to the extent authorized under the Privacy Act and Freedom of Information Act. Further, individuals generally may not correct or amend their PII in systems that contain inquiry and investigative 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).

	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO): **If an ATO has not been completed, but is underway, provide status or expected completion date:** The ATO process is in progress but the expected issuance is yet to be determined. **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:** The Privacy controls related POA&M related to processing this document and Privacy Impact Assessment if determined to be required. Once these documents are completed, the PO&AM will be closed.
X	ATO is in progress. Authority to Proceed (ATP) is pending CISO review and approval.
	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:
	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: The information types have designated this system to be a High impact system.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Once an ATO is issued, DOJ core controls are evaluated yearly. Continuous monitoring will be conducted, and Privacy controls will be implemented and assessed within the Joint Cybersecurity Authorization Management (JCAM) system through the ATO process. DEA will also monitor the information system on a continuous basis for changes to the information system or its operational environment, the information system security and privacy plan boundaries, or other conditions. DEA conducts security impact analyses of system associated changes, update of the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the DOJ CPCLO (Chief Privacy and Civil Liberties Officer), or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
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:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) will be responsible for reviewing and analyzing the on-prem UEM information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with DEA Incident Response Plan. DEA TCVV monitors on-prem assets using the Splunk event correlation tool to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Remedy ticketing system.
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**. As a standard operating procedure, all contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.
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: Required training is distributed and tracked via the DOJ Learning Management System, DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and Cyber Security awareness training that are applicable to all DEA component personnel. However, the Office of Chief Counsel (OCC) is deploying a role-based, annual privacy training which should be required for DEA personnel in FY2025.

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?

As required by the Authorization to Operate process, Ontic will involve the implementation and maintenance of numerous physical, technical and administrative privacy and security controls:

Physical privacy and security controls:

Physical access control measures are in place to protect the data and will be tested for both IST's and ISE's instances of the system. Both instances will be subject to audit by the Office of Inspections. Ontic has been deployed in a DEA secured data center. This data center provides physical protection for all hosted systems to include servers, switches, and other devices employed to support the DEA mission. In addition, the data center supplies electrical and HVAC systems for the hosted components. The data center utilizes numerous safeguards to include guards who monitor the facility. Entry includes two sets of doors, the first utilizes your Personal Identity Verification (PIV) Card which is scanned for entry. The second door requires use of the PIV as well as the associated individual PIN. Cameras have been deployed at critical locations to include entry ways. Metal Detectors have been employed for any visitors that do not have a PIV. All physical controls for Ontic are inherited from the data center.

Technical privacy and security controls:

Through the utilization of specific access controls and data protection techniques deployed, access to this data is controlled by system administrators and authorized personnel that have a need to know based on their job duty and position within the organization. This information is used to create access controls and separation of duty. The Ontic application components utilize the following technical controls to protect the data:

- Database encryption for data at rest
- Disk Encryption
- Transport Layer Security (TLS) for data encryption in transit
- Data Loss Prevention (DLP) software

Administrative privacy and security controls:

Numerous processes/controls have been implemented by DEA to ensure collected data is required, and relevant. These processes include:

- Identifying and selecting the following types of information system accounts to support organizational missions/business functions: individual, group/shared, service, guest/anonymous, and temporary/emergency accounts;
- Assigning account managers for information system accounts;
- Establishing conditions for group and role membership;
- Specifying authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requiring approvals by for requests to create information system accounts;
- Ensuring the system creates, enables, modifies, disables, and removes information system accounts in accordance with DOJ Order 0904: Cybersecurity Program and applicable information system policy and procedures;
- Monitoring the use of information system accounts;
- Notifying account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes;
- Authorizing access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions;
- Reviewing accounts for compliance with account management requirements.

Additionally, the administrative controls include applicable DOJ and DEA IT Rules of Behavior and other applicable privacy and cybersecurity policies including on password management and incident response; workforce training on privacy and cybersecurity; and assigning users access consistent with need-to-know. ISE and IST personnel are also required to attend supplemental privacy and security training, including Cyber Security Awareness Training. IST personnel take DOJ cybersecurity assessment training (CSAT) annually

Further, security and privacy control compliance will be subject to regular review by ISE and IST management and audit by the Office of Inspections, and coordination with Office of Chief Counsel. As standard operating procedure, the Office of Acquisition & Relocation Management (FA) includes in contracts Privacy Act clauses, including those required by DOJ, in contracts awarded.

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.)

ISE – See DAA-0170-2017-0007, Inspections Records, including DEA Employee Security Files Disposition Authority Number DAA-0170-2017-0007-0002: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0170/daa-0170-2017-0007_sf115.pdf,

- Records reflecting attacks or threats of attacks against DEA employees, facilities, and assets including acts of terrorism. May include, but not limited to: transcripts, reports, violations, and correspondence.
- This schedule provides for a retention period of 5 years after cutoff (absent another applicable schedule, e.g. if an incident, or a shooting, or other applicable circumstances as described in DAA-0170-2017-0007).
- For investigative case tracking, for files relating to those activities of drug/narcotic enforcement pertaining to criminal/regulatory investigations, drug abuse prevention, and other enforcement-related operations, see DFN 601-39 (DAA-0170-2013-0004-0001) (Supersedes DFN 601-07 and DFN 601-08). See: https://intranet13.shpt.sbu.dea.doj.gov/sites/sa/sarr/dearis/Pages/App600.aspx)

IST – See General Records Schedule (GRS) 5.6, for full details on Security/Insider Threat Program records retention periods: https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs-2017-0006_sf115.pdf?_ga=2.120482056.1866381034.1692041441-1538916692.1662480111

- DEA uses the DFN 260 series for the Insider Threat records schedules outlined in the GRS.
- Depending on the specifics, different retention periods can apply; GRS 5.6 and DFN 260 provide for 25 years for insider threat inquiry records though longer retention is authorized if required for business use. See: https://intranet13.shpt.sbu.dea.doj.gov/sites/sa/sarr/dearis/Pages/App200.aspx

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:

ISE:

- DOJ-011, *Access Control System*, 69 Fed. Reg. 70279 (Dec. 03, 2004)(full text); 82 Fed. Reg. 24147 (May, 25, 2017)(amendment). https://www.gpo.gov/fdsys/pkg/FR-2004-12-03/pdf/04-26590.pdf
- DOJ-020, *DOJ Identity, Credential, and Access Service Records System,* 84 Fed. Reg. 60110 (Nov. 7, 2019)(full text); https://www.govinfo.gov/content/pkg/FR-2019-11-07/pdf/2019-24246.pdf
- DEA-008, *Investigative Reporting and Filing*, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May, 25, 2017)(amendment). https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf
- DEA-010, *Planning and Inspection Division Record*s, 52 Fed. Reg. 47182, 213 (Dec. 11, 1987)(full text); 66 Fed. Reg. 8425 (Jan. 31, 2001); 82 Fed. Reg. 24147 (May, 25, 2017)(amendments). https://www.justice.gov/opcl/docs/52fr47182.pdf
- DEA-013, *Security Files,* 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)(full text); 66 Fed. Reg. 8425 (Jan. 31, 2001); 82 Fed. Reg. 24147 (May, 25, 2017)(amendments). https://www.justice.gov/opcl/docs/52fr47182.pdf

IST:

- DOJ-002, *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, 86 Fed. Reg. 37188 (Jul. 14, 2021)(full text). https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf
- DOJ-006, *Personnel Investigation and Security Clearance Record for the Department of Justice*, 67 Fed. Reg. 59864 (Sep. 24, 2002)(full text); *69 Fed. Reg. 65224 (11-10-2004); 82 Fed. Reg. 24147 (May, 25, 2017) (amendments).* https://www.gpo.gov/fdsys/pkg/FR-2002-09-24/pdf/02-24206.pdf
- DOJ-018, *DOJ Insider Threat Program Records,* 82 Fed. Reg. 25812 (Jun. 05, 2017)(full text); 82 Fed. Reg. 27872 (Jun. 19, 2017)(correction). https://www.gpo.gov/fdsys/pkg/FR-2017-06-05/pdf/2017-11445.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?

a. Potential Threats Related to Information Collection

Privacy Risk: Potential for overcollection of unnecessary PII

Mitigation: This risk is mitigated. IST and ISE personnel are trained law enforcement officers skilled in conducting proper law enforcement investigations and collecting only the relevant

evidence necessary to assess insider threats and to protect DEA's workforce and facilities. For instance, ISE collects PII only to the extent required for their mission and functions of protecting the DEA workforce and DEA facilities. ISE personnel are also subject to the direction and oversight of the Chief Inspector and follow the strictures of the DCI Security Programs.

Similarly, PII for IST use will be collected as directed by E.O. 13587, the mandates of the November 21, 2012 Presidential Memorandum setting out minimum standards for insider threat programs, best practices from the DOJ Insider Threat Working Group and other government entities with expertise and authority in this area (including the National Counterintelligence and Security Center), the direction of the Chief Inspector (DEA's Senior Insider Threat Official), and the DCI Security Programs (DEA's Alternate Insider Threat Official) as described in the Inspection Manual Section 8811. To the extent that targets of investigations or inquiries are determined not to be a potential threat, the information will be retained according to retention schedules, but in a closed case file. Further, during inquiries or investigations, data sources can and will be removed to the extent determined unnecessary.

Privacy Risk: Some PII collected may not be directly relevant and necessary for the DEA to accomplish its purpose/mission.

Mitigation: This risk is mitigated. To the extent that some PII collected is not directly relevant and necessary for the system to accomplish its purpose/mission, it will be kept according to records retention schedules, however, only in case files which are administratively closed. While the analytics system will have access to DEA internal systems, only those patterns suggestive of a possible insider threat would come to the attention of IST for further internal analysis to rule out or identify a possible issue. Likewise, to the extent that PII about an individual is collected but they are ruled out as a potential threat, the information will be retained according to retention schedules, but in a closed case file.

Privacy Risk: The system could be used to improperly collect images of or the content from the exercise of protected First Amendment activities

Mitigation: This risk is mitigated. It is a reality that threat activity can occur on social media, which also includes protected First Amendment activity. However, when members of the public post on the open internet, the communications may also be viewed by anyone. For any investigative activities requiring a warrant, judicial process determined that the applicable standards were met for collection of the PII.

In addition, physical security threats such as intrusions into federal buildings can occur in conjunction with an activity such as a protest but at the same time violate applicable federal law, federal building regulations and physical and information security requirements.
To the extent that First Amendment activities arise in the course of IST activities, inquiries are conducted in accordance with best management practices and Office of Chief Counsel coordination for protection of civil rights and civil liberties. IST and ISE work in coordination with Office of Chief Counsel to ensure that activities are consistent with legal authorities and the Constitution. Likewise, ISE's agents can coordinate with Office of Chief Counsel as

needed for legal advice related to civil rights and civil liberties. No information will be collected solely on the basis of protected First Amendment activity.

Privacy Risk: By aggregating data from many systems and data sources, DEA may exceed the minimal amount of data necessary to satisfy ISE's mission of protecting DEA's workforce and facilities or IST's counter-insider threat mission.

Mitigation: This risk is mitigated. ISE will collect PII only to the extent authorized and necessary for ISE to protect DEA's workforce and facilities, consistent with the direction and oversight of the Chief Inspector and the DCI Security Programs, and in coordination with Office of Chief Counsel for legal advice as appropriate.

With respect to IST, PII will be collected as authorized by EO 13587, the mandates of the November 21, 2012 Presidential Memorandum setting out minimum standards for insider threat programs, best practices from the DOJ Insider Threat Working Group and other government entities with expertise and authority in this area (including the National Counterintelligence and Security Center), and the direction of the Chief Inspector (DEA's Senior Insider Threat Official) and the DCI Security Programs (DEA's Alternate Insider Threat Official) as described in the Inspection Manual Section 8811. Data sources will be removed to the extent determined unnecessary.

Privacy Risk: possibility that the PII of an unrelated individuals who are not under suspicion or the subjects of inquiries may be collected as part of an incident, inquiry or investigation about someone else.

Mitigation: This risk is mitigated. Personnel may encounter sensitive PII and PHI of unrelated individuals through system monitoring or reviewing artifacts under review in inquiries of possible improper disclosures, however, IST personnel receive supplemental training in privacy and security fundamentals and in-office work takes place in a SCIF. Because IST's work is centered around system monitoring and prevention and detection of insider threats, the systems and information drawn into IST's use of Ontic comes mainly from within existing DEA information collected for investigatory or internal governmental purposes, limiting the extent to which the PII of individuals unrelated to DEA purposes is at issue. The same timeliness and accuracy provisions would apply to Ontic data as the underlying DEA information. The system will be updated as underlying source records are updated, and so will be kept equally up to date as the underlying source records. Also, many of the internal governmental records are generally subject to a right of access and amendment to help ensure accuracy.

With respect to ISE, its Ontic information encompass many individuals for whom a threat assessment necessarily must be made and some of whom will be determined not to be an actionable threat. To the extent that PII about an individual is collected but they are ruled out as a potential threat, the information will be retained according to retention schedules, but in a closed case file.

b. Potential Threats Related to Use and Maintenance of the Information

Privacy Risk: Some PII may be used for a purpose or in a manner unrelated to the reason why the information was collected or for unapproved/inappropriate purpose (such as searching for, or creating records or lookouts for friends, relatives, neighbors, the users themselves, or celebrities and other members of the public).

Mitigation: This risk is mitigated. DEA personnel are trained to use the PII only to the extent consistent with the purpose of its collection. Much of the insider threat information in Ontic comes from within DEA personnel background and investigation files that can be clearly connected to the insider threat prevention and detection uses consistent with ISE's authorities, pursuant to management direction and oversight of the Chief Inspector and DCI Security Programs, with advice from Office of Chief Counsel as appropriate.

In addition, the number of users within the DEA Inspections Division is limited and is subject to management oversight. Access is limited to a small group of trained and carefully supervised employees. ISE will access the system within secure office space limited to ISE and/or on secure Firebird systems. ISE's use will be subject to system monitoring to which all users agree and which is conducted by IST. Use of the system is also subject to system monitoring and routine audit and inspections by the Inspections Division. The system will also include audit trail features and a mechanism allowing production of documents as required for FOIA purposes. Further, both ISE and IST will have supplemental security and privacy training for users.

Privacy Risk: PII could be accessed for unapproved or inappropriate purposes (such as searching for, or creating records or lookouts for friends, relatives, neighbors, the users themselves, or celebrities and other members of the public.

Mitigation: This risk is mitigated. IST's use of the Ontic case management system will be limited to authorized users. This usage is subject to management oversight including by the Chief Inspector and DCI Security programs, and in coordination with the Office of Chief Counsel. Technical controls on the system include that the system stores records collected for audit trails, and to enable processing of FOIA requests submitted to DEA. Additionally, all IST and ISE personnel sign IT Rules of Behavior and take privacy training making clear DEA information is to be used only for official purposes.

Privacy Risk: Physical, technical or administrative security and privacy controls, such as access controls, may be insufficient to safeguard PII from outside penetration or breach attempts.

Mitigation: This risk is mitigated. DEA deploys the physical, technical and administrative security and privacy controls as set forth in Section 6.2 to safeguard this system which are subject to review and should be effective in protecting the system. Technical controls on the system include PIV authentication. Administrative controls include system storage of system use collected for audit trails, and to enable processing of FOIA requests submitted to DEA. There are additional requirements to access the system within a SCIF and/or on secure Firebird systems. These controls include authorizing only a limited number of users. The

system users will be limited to the members of two discrete programs, ISE and IST, and a limited number of support and oversight personnel who are subject to an approval process. Additionally, ISE and IST personnel receive supplemental security and privacy training.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Potential for DEA personnel to share or disclose PII Information to an inappropriate party or for an improper use or in a manner inconsistent with a routine use in the relevant SORN (specify) or DEA/DOJ policy.

Mitigation: This risk is mitigated. Initial access to Ontic data is restricted to a limited number of authorized government personnel. Disclosure/dissemination policies are in place to limit who can receive this data, including as specified in applicable SORNs and the DEA Agents Manual providing for the use of a DEA-381 form to document each disclosure of investigative information outside of DEA. Additionally, permission-based access is set in place to restrict access to the data. Authorized IST and ISE personnel also will receive supplemental security and privacy training and can consult management and Office of Chief Counsel for legal advice as appropriate.