Drug Enforcement Administration

Privacy Impact Assessment
for the
Remote Analysis Viewing and Notation System (RAVANS)

Issued by:

James Robert Bryden,
DEA Senior Component Official for Privacy

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

Date approved: February 27, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

The Remote Analysis Viewing and Notation System (RAVANS) is a system controlled and maintained by the Drug Enforcement Administration (DEA) that is used by Special Agents (SAs), Diversion Investigators (DIs), Task Force Officers (TFOs), and Intelligence Analysts (IAs) to collect court-authorized or consensual historical electronic data in connection with criminal investigations. Depending on the information sought, the DEA may be authorized to obtain historical electronic data through Search Warrants, 18 U.S.C. § 2703d Court Orders, Administrative Subpoenas, and Grand Jury Subpoenas, or with the consent of the individual.

Much of the historical electronic data in RAVANS is generated by the subjects of the criminal investigations who utilize electronic devices or service-provider products to facilitate violations of the Controlled Substances Act (CSA), Title 21 United States Code (U.S.C.) and associated federal crimes. Data may be obtained from lawfully seized electronic devices such as computers and cell phones; it also may be obtained from service providers in the commercial market. Data may include email content and metadata, device backup data, SMS (text) and MMS (multimedia) messages, as well as other types of text-based communications over social media platforms. The metadata in RAVANS may include communication dates and times as well as participant identifiers (usernames, account numbers, phone numbers, email addresses, and Internet Protocol (IP) addresses).

Pertinent data in RAVANS is often used as evidence in criminal, civil, or administrative court proceedings to seize assets that were derived from drug trafficking. When RAVANS receives, processes, and delivers content and metadata in connection with legal process, it makes it available to DEA investigative teams in accordance with the evidence-handling requirements specified by the legal authority responsible for issuing that legal process.

Whatever type of data is involved, RAVANS utilizes the principle of "least privilege" to restrict access to those personnel with a need to know, on both the database and application layers. Roles are designated to ensure users view only the appropriate data subsets for which they are permitted. Physical components of the RAVANS system are stored in access-controlled areas restricted to all but authorized personnel.

Information contained within RAVANS includes information in identifiable form about non-Government personnel necessitating DEA complete this Privacy Impact Assessment, in accordance with Section 208 of the E-Government Act of 2002.

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.

DEA investigations target illicit drug trafficking organizations and associated individuals who frequently utilize electronic means to communicate regarding their illicit activities and conduct. In the course of an investigation, data is generated by the subjects of the criminal investigations who utilize electronic devices or service-provider products to facilitate violations of the CSA. Data in RAVANS is obtained in several ways. Data may come from lawfully seized devices such as computers and cell phones; or it is obtained from information technology service providers in the commercial market. Data may also be obtained via the consent of the individual user or consumer of the data. The type of data collected may be comprised of (but not limited to) email content and metadata, device backup data, SMS (text) and MMS (multimedia) messages, or other types of text-based communications over social media platforms. The types of metadata obtained may include communication dates and times as well as participant identifiers (usernames, account numbers, phone numbers, email addresses, and Internet Protocol (IP) addresses). Historical data may be obtained through a variety of legal processes including search warrants, court orders, administrative and Grand Jury subpoenas, and through consent of the user. Data is obtained and analyzed in order to gather evidence for prosecution and to create additional investigative leads. Such data also is helpful in identifying Drug Trafficking Organization members and in determining the degree to which they conspire with one another to commit criminal acts in violation of the CSA.

Title II of the Electronic Communications Privacy Act of 1986 (ECPA), as amended, the Stored Communications Act (SCA),18 U.S.C. § 2701, et seq., protects the privacy of the contents of files stored by service providers and of records held about subscribers by service providers, such as subscriber name, billing records, or IP addresses. Pursuant to the SCA, non-content, historical data (data that has been stored for 180 days or longer) such as subscriber name and address, local and long-distance telephone connection records, or records of session times and durations, length and types of service, telephone/instrument number or other subscriber number/identity, and/or payment information may be lawfully obtained via Administrative or Grand Jury Subpoena under 18 U.S.C. § 2703(c); the government must establish that the data sought is relevant and material to the investigation. Additional non-content, historical data including other records or information pertaining to a subscriber may be obtained pursuant to a court order under 18 U.S.C. § 2703(d). For all historical data, except extended, continuous mobile phone location information, the government must establish specific and articulable facts as to why the information sought is relevant and material to the investigation to obtain the court order; but for extended, continuous location information of the mobile phone user, the government must demonstrate the same probable cause necessary to seek a search warrant, unless an established exception to the warrant requirement is applicable.

Under Rule 41 of the Federal Rules of Criminal Procedure, and the SCA, the government may petition the court to lawfully obtain electronic content and metadata generated or related to the target of an investigation. See 18 U.S.C. § 2701, et seq. Prior to the issuance of a search warrant, the government must establish probable cause, which details the pertinent facts of the investigation as well as the potential value of the electronic evidence being sought. Once the search for data which meets the requirements of the search warrant has been conducted, only data which is determined to be responsive to the search warrant is retained and accessible to the investigative team. Any data deemed non-responsive that is maintained as a record within RAVANS is marked and siloed in a manner that is inaccessible to the investigative team. Responsive data is provided to the investigative team for further investigation and use as evidence as appropriate.

Finally, search and seizure of data in an investigation may occur pursuant to the consent of the user or consumer of the data. In these cases, the scope of the consent provided (e.g., within a certain date range or limited to specific keywords or media) dictates the limits of the government's authority to search and seize the data. Consent of the individual is needed for both the search as well as the seizure of the electronic data. Consensually obtained data is processed by RAVANS, and shared and used, in the same fashion as data obtained through court authorization—that is, only members of the investigative or prosecution team have access to the data. Physical evidentiary copies of the data are provided to a designated individual of the respective investigative team, to be stored in a DEA Non-Drug evidence vault located at each field office.

Due to the various formats and volume of data received through the various legal processes mentioned above, it is necessary for DEA to have an information system that is capable of receiving, processing, and presenting communications and associated data in a readable and useable format for agents and investigative teams to review and make determinations as to the relevance and materiality of the data to the investigation. RAVANS serves this function by possessing numerous analytic functions, including conducting reviews of the lawfully obtained data and making determinations as to relevance and responsiveness to the search warrant terms, translating and/or transcribing the content of communications, archiving evidence, and producing material in discovery to the defendant in accordance with the Federal Rules of Criminal Procedure and DOJ Policy. Data maintained in RAVANS is not shared with the public and is only distributed to and utilized by members of the investigative or prosecution team.

Data Collection

Historical data obtained from a service provider pursuant to a search warrant, court order, or administrative or Grand Jury subpoena must be transferred from the provider to the investigative team. When a service provider is served legal process authorizing the release of data, the provider processes the request or demand according to their methods by conducting a review of their historical records and facilitating the transfer of the outlined content and metadata to DEA. Most commonly, the service provider transfers data via a secure download process which consists of two steps: 1) the service provider sends DEA a Hyper Transfer Protocol Secure (HTTPS) which is accessed by 2) a password that is separately provided by the service provider.

In rare cases, the data may be delivered as a password protected disc or drive by certified mail from the provider.

Consensually obtained data is processed by RAVANS and shared and used in the same fashion as data obtained through court authorization. Evidentiary copies of the data are provided to a designated individual of the respective investigative team, to be stored in a DEA Non-Drug evidence vault located at each field office.

Data Processing

RAVANS accepts stored data in many different formats from service providers. In the rare occasion when data is in a format that cannot be accepted directly into the analytical application, the data is normalized by DEA into a standard, readable format. The data can then be properly viewed by authorized users for review and analysis. The original provider data set is maintained and stored as evidence by the investigative team.

Data Use

Data within RAVANS is indexed and retrieved by communications identifiers such as phone numbers, email addresses, IP addresses, and other markers used when transmitting and receiving communications. Only members of the investigative or prosecution team who are granted access to RAVANS and the particular data set may conduct a search of the data; the search is limited by case. Data may also be searched for and retrieved using keywords in the viewing and analysis tools. Keyword searches are performed for both communication metadata and content. Keyword searches and data retrieval are limited in scope to data that the user is authorized to access per their respective roles. The system can produce evidentiary exhibits for presentation by law enforcement officials in courts of law. These exhibits can be reports or exports that can be printed or saved to external media and are provided to defense counsel in the evidentiary discovery process.

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	The Comprehensive Drug Abuse Prevention and Control Act of 1970 (Controlled Substances Act), 21 U.S.C. § 801 et. seq., (In particular, 21 U.S.C. §§ 878-880), and its attendant regulations (21 C.F.R. § 1300, et seq.); See also, 18 U.S.C. §2703, 40 U.S.C. § 11101, 44 U.S.C. § 3502,
Executive Order	
Federal regulation	
Agreement, memorandum of understanding, or other documented arrangement	

Authority	Citation/Reference
Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. 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 and D	Names of members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Names of employees, contractors, detailees and/or other federal govt. personnel, should arise infrequently.
Date of birth or age	X	A, B, C and D	**Note**: Hereinafter asterisks indicate that intercepted communications by targets and members of the public (US or non-USPERs) could include any type of content. Not all of these types of information are routinely contained in communications. Such information for employees, contactors, detailees and other federal personnel should arise infrequently.
Place of birth	X	A, B, C and D	*
Gender	X	A, B, C and D	*
Race, ethnicity, or citizenship	X	A, B, C and D	*
Religion	X	A, B, C and D	*
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	*
Tax Identification Number (TIN)	X	A, B, C and D	*

(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
Driver's license	X	A, B, C and D	*
Alien registration number	X	A, B, C and D	*
Passport number	X	A, B, C and D	*
Mother's maiden name	X	A, B, C and D	*
Vehicle identifiers	X	A, B, C and D	*
Personal mailing address	X	A, B, C and D	*
Personal e-mail address	X	A, B, C and D	E-mail addresses of members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Such information for employees, contractors, detailees, and other federal personnel should arise infrequently
Personal phone number	X	A, B, C and D	Phone numbers of members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Such information for employees, contractors, detailees, and other federal personnel would arise infrequently.
Medical records number	X	A, B, C and D	*
Medical notes or other medical or health information	X	A, B, C and D	*
Financial account information	X	A, B, C and D	*
Applicant information	X	A, B, C and D	*
Education records	X	A, B, C and D	*
Military status or other information	X	A, B, C and D	*
Employment status, history, or similar information	X	A, B, C and D	*
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	*
Certificates	X	A, B, C and D	*
Legal documents	X	A, B, C and D	*
Device identifiers, e.g., mobile devices	X	A, B, C and D	Device identifiers of members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Such information for employees, contractors, detailees, and other federal personnel would arise infrequently.

(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
Web uniform resource locator(s)	X	A, B, C and D	Such locators for members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Such information for employees, contractors, detailees, and other federal personnel would arise infrequently.
Foreign activities	X	A, B, C and D	*
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	*
Juvenile criminal records information	X	A, B, C and D	*
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	*
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C and D	*
Grand jury information	X	A, B, C and D	*
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	*
Procurement/contracting records	X	A, B, C and D	*
Proprietary or business information	X	A, B, C and D	*
Location information, including continuous or intermittent location tracking capabilities		A, B, C and D	Location information of members of the public (US or non-USPERs) could be collected specific to an investigation or incidentally collected. Such information for employees, contractors, detailees, and other federal personnel would arise infrequently.
Biometric data:	X	A, B, C and D	*
- **Photographs or photographic identifiers**	X	A, B, C and D	*
- **Video containing biometric data**	X	A, B, C and D	*
- **Fingerprints**	X	A, B, C and D	*
- **Palm prints**	X	A, B, C and D	*
- **Iris image**	X	A, B, C and D	*
- **Dental profile**	X	A, B, C and D	*
- **Voice recording/signatures**	X	A, B, C and D	*
- **Scars, marks, tattoos**	X	A, B, C and D	*

(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
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	*
- **DNA profiles**	X	A, B, C and D	*
- **Other (specify)**	X	A, B, C and D	*
System admin/audit data:	X	A, B, C and D	Multiple types of administration and audit data are maintained for employees, contractors, detailees, and other federal personnel.
- **User ID**	X	A, B, C and D	See note above
- **User passwords/codes**	X	A, B, C and D	See note above
- **IP address**	X	A, B, C and D	See note above
- **Date/time of access**	X	A, B, C and D	See note above
- **Queries run**	X	A, B, C and D	See note above
- **Contents of files**	X	A, B, C and D	See note above
Other (please list the type of info and describe as completely as possible):	X	A, B, C and D	Any electronic communications and metadata generated by a target that falls within the scope of the court order or consent will be stored.

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		Online	X
Phone		Email			
Other (specify): Consensual searches are primarily conducted in-person with the individual to whom the information pertains. However, because it may be necessary to log-in to the individual's account, with their consent and in their presence, "Online" is also marked.					

Government sources:					
Within the Component		Other DOJ Components		Other federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): RAVANS does receive information from State or local police, but only to the extent State or local police have been deputized as a DEA Task Force Officers. Thus, the state, local, tribal box is not checked due to the fact that these TFOs are under DEA supervision.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	x
Commercial data brokers					
Other (specify): Data collected through legal process from a service provider or seized electronic device. The data is generated by the target of the investigation or by individuals communicating directly with the target, through their use of communication platforms.					

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	RAVANS system administrators may view the data in limited instances when technical system issues arise in order to provide troubleshooting. Information sharing of intercepted data within DEA is limited to DEA task force officers and employees who have a legitimate need for the record in the performance of their duties. DEA investigative teams use the data as evidence on a case-by-case basis. If evidence obtained in a case is relevant to a different investigation, that evidence may be shared with investigators working on the second investigation, consistent with the guidelines of the issued court order and Federal Privacy Laws.
DOJ Components	X			Information sharing of intercepted data within DOJ is limited to DOJ officers and employees who have a

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.**
				legitimate need for the record in the performance of their duties. Information in this system may be shared with U.S. Attorneys in relevant operations/ prosecutions/ cases. Data may be shared, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation.
Federal entities	X			Data may be shared, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation. Data may also be shared as part of the routine uses described in the System of Record Notices described in Section 5.1 below.
State, local, tribal gov't entities	X			Data may be shared, within legal guidelines, in joint cases with other law enforcement entities. In limited instances, the data may be shared with law enforcement entities who are conducting criminal investigations, where the data is relevant to a separate investigation.
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	X			Data is shared as part of the evidentiary discovery process and may be presented in a court of law as evidence.
Private sector				
Foreign governments	X			Data is shared only if a Mutual Legal Assistance Treaty (MLAT) has been signed and is in place.
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 from RAVANS will not be released to the public for "open data" purposes.

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.

General notice of collection, use, and sharing is provided by:

- JUSTICE/DEA-008, "Investigative Reporting and Filing System" 77 Fed. Reg. 21808 (April 11, 2012);
- JUSTICE/DEA-011, "Operations Files," 52 Fed. Reg. 47182, 47214 (Dec. 11, 1987);
- JUSTICE/DEA-INS-111, "Automated Intelligence Records System (Pathfinder)." 55 Fed. Reg. 9148, 49182 (Nov. 26, 1990); and

- JUSTICE/DEA-022, "El Paso Intelligence Center (EPIC) Seizure System (ESS)" 71 Fed. Reg. 36362 (June 26, 2006).

Pursuant to the SCA, the government must provide notice to a subscriber when it uses a subpoena or 2703(d) court order to obtain the contents of the subscriber's stored communications. This notice may be delayed when the notice may have an adverse result as defined in the SCA. See 18 U.S.C. § 2705(a). No notice is required to be provided by the government to the subscriber, however, when it uses an administrative or grand jury subpoena or 2703d order to obtain non-content, subscriber or other records in accordance with 18 U.S.C. § 2703. Additionally, no notice is required to be provided by the government to the subscriber when a search warrant is issued upon a service provider to obtain the contents of the subscriber's stored communications, in accordance with 18 U.S.C. § 2703.

Upon receipt of a demand for legal process from the government, a service provider may provide notice to the subscriber. However, the SCA also allows the government to seek a non-disclosure order from the service provider to subscriber where said notice will result in adverse results; see 18 U.S.C. § 2705. Similarly, in the conduct of executing a Federal Rule of Criminal Procedure, Rule 41 search warrant, notice is required to be provided to the owner of the property being searched. Again, however, delay of notice may be sought where there is reason to believe notification will result in adverse results; see 18 U.S.C. § 3103a.

Notice to individuals is further offered through criminal legal process and procedure. Under the Federal Rules of Criminal Procedure, Rule 41, the officer executing the warrant must provide a copy of the warrant and generate a receipt for the property taken from the person, in the case of RAVANS, digital evidence. Additionally, the officer must return the served warrant to the issuing court, along with the receipt of the lawfully seized items. Upon request, the issuing judge must provide a copy of the warrant and receipt of the seized items to the person with the legal standing.

In the criminal discovery process, all relevant and material evidence is provided to the defendant to aid in their defense. In the case where someone has communicated with a defendant and the party has not been formally charged, they will not receive notice that their communications were lawfully obtained though the defendant's account. Each SORN listed above is exempt from notification requirements by 28 C.F.R. § 16.98. If the data is not responsive to the legal process, the data will be marked and siloed to prevent further access.

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.

A person who is cooperating with law enforcement and consents to the search and/or seizure of their electronic data may voluntarily participate in the collection and use information within the system and choose to allow their data to be collected as evidence. This process is referred to as a consent. As described above, the scope of any search and/or seizure of an individual's data is directly limited by the individual's terms of consent.

Parties whose digital content and metadata are seized pursuant to lawful process do not have an

opportunity to decline the collection, use, or dissemination of information in RAVANS. If formally charged, the parties whose data was collected as evidence have the right to challenge the accuracy of the collected information in their defense, as well as the manner and means by which the information was collected.

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.

DEA's public facing website contains a FOIA/PA webpage which provides members of the public with instructions for filing a request for access to information about themselves to DEA. The FOIA/PA website also contains procedures for filing a request for record correction or amendment to DEA.

Insomuch as the information contained in RAVANS is a copy of the data contained as evidence in the active casefile, the Federal Rules of Criminal Procedure require that a defendant be provided a copy of the evidence that will be used in a court proceeding against them, as well as items that are relevant and material to the defense. The prosecuting attorney will coordinate the discovery of any relevant and material evidence, including intercepted communications and associated metadata, to the defendant's legal counsel.

Individuals whose communications are collected and who are not prosecuted will not gain access to the information in RAVANS pertaining to them. Information obtained from the use of RAVANS is retained in DEA's Investigative Reporting and Filing System (and other listed systems) and have been exempted from disclosure, amendment, and correction elements pursuant to 28 C.F.R. §16.98. Records compiled for law enforcement purposes are also excluded from production under the Freedom of Information Act (FOIA). 5 U.S.C. §552(b)(7).

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):
	ATO expires on June 30, 2024.
	If an ATO has not been completed, but is underway, provide status or expected completion date: N/A
X	**Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs)**

	for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation: This information is sensitive.
	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:** RAVANS enables capabilities for enhancement of digital criminal investigations, including but not limited to: • Manage large amounts of communication data legally obtained from subject devices and associated accounts • Ingest, parse, and analyze text messages, phones calls, images and GPS data from devices • Analyze social media data and conversations from various technology platforms in their proprietary file formats • Provide integrated user interface for historical analysis of phone, social media, tower, cell phone forensic, and email data
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: All data is hashed upon loading into RAVANS to ensure no data has been manipulated. RAVANS internal audit log shows who, when and what was marked by investigators.**
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:** Account auditing is performed every 60 days to ensure access is still required. Account holders are also automatically required to change their password every 90 days. If the password is not changed, it will automatically be disabled.
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:** The vendor of the analytical application offers training material in the use of the application if it is needed.

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?

Computer login restrictions permit only authorized users access to the data. Data is also protected by permission-based restrictions at both the application interface and the file level. The system is accessed by users with unique and attributable accounts within government facilities. RAVANS utilizes role-based permissions for accessing data and system components. The level of access is determined by the user's role on the system and is limited to the degree needed to fill the role. System administrators also access the system using unique and attributable accounts as well as ability to access via a VPN connection and a two-factor authentication process. Data within the system is encrypted at rest; and users have remote access to the server.

RAVANS data is protected from unauthorized viewing and copying by physical access restrictions. The RAVANS server is located in a secure government facility to which only authorized individuals have access. Further, the system is located in a restricted room within the building, again, to which limited authorized personnel with a need to have access may gain entry. General users can access the system in DEA controlled spaces that are approved work areas. The areas have control measures to document and limit access to only authorized users of the system. Both general users and system administrators can also gain remote access to the system. The areas have control measures to document and limit access to only authorized users of the system. Access history of the physical workspaces is logged and access to RAVANS and the separate data sets is also logged and maintained.

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.)

RAVANS data is generally downloaded into the relevant investigative case file and is retained in accordance with DFN 601-39c1, DEA IMPACT Numbered Case Files, which directs, "cut off at the close of case and destroy/delete 25 years after case closed." However, retention periods for the RAVANS data in the casefile will be different than the data stored on RAVANS itself (which will be duplicative of the data that goes to the casefile). Data retained in RAVANS is retained according to DFN 601-38a2 that directs, "cutoff at the close of the file annually and destroy 2 years after close of file." Any data deemed non-responsive maintained as a record within RAVANS that had been marked and siloed in a manner that was inaccessible to the investigative team would not be retained after case closure.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizen s 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:

- DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf.
- JUSTICE/DEA-011, "Operations Files," 52 Fed. Reg 47182 47214 (Dec. 11, 1987) (https://www.justice.gov/opcl/docs/52fr47182.pdf);
- JUSTICE/DEA-INS-111, "Automated Intelligence Records System (Pathfinder)." 55 Fed. Reg. 49148, 49182 (Nov. 26, 1990) (https://www.justice.gov/opcl/docs/55fr49146.pdf); and
- JUSTICE/DEA-022, "El Paso Intelligence Center (EPIC) Seizure System (ESS)" 71 Fed. Reg. 36362 (June 26, 2006)(https://www.govinfo.gov/content/pkg/FR-2006-06-26/pdf/E6-9977.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 the Collection of Information

Privacy Risk: Over-collecting and maintaining more personal information than necessary to accomplish DEA's official duties and its mission.

Mitigation: This risk is partially mitigated. There is some data minimization applied with this system regarding permitting access only to information responsive to legal process. The lawfully collected data is initially reviewed for responsiveness to the court order. Data that is not responsive is marked and the data is systematically not visible to the investigative team. The data is still kept within RAVANS. All data is deleted upon case closure.

Privacy Risk: DEA may collect PII for investigations or activities beyond the scope of its Title 21 authority.

Mitigation: This risk is mitigated. The DEA must always demonstrate its authority and justification for the collection in the process to obtain court authorizations. Prior to each lawful seizure, the investigating agent and the assigned prosecutor outline the items to be seized and the nature of the information that is sought as well as the Title 21 authority for DEA to obtain the information sought. These details are enumerated in the affidavit to the court. Agency policy also requires supervisory approval before beginning an investigation wherein any Title 21 authority issues would be addressed.

Further, to the extent any information collected is not responsive to the issued search warrant, it is siloed from the investigative team and only the relevant information may be used in the investigation. This is done to limit the level of privacy intrusions on the subject, while still allowing law enforcement to pursue the investigation.

Privacy Risk: The system could be used to improperly collect images of or communications that are themselves an exercise of protected First Amendment activities.

Mitigation: This risk is mitigated. DEA operates under guidelines that restrict the collection of records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by law or pertinent to and in scope of authorized Law Enforcement activity. DEA has a special approval process for any "enforcement procedures" that are considered "sensitive investigative activities," such as operations involving a religious or political organization or the activities of the news media to ensure sufficient oversight in the event of such an investigation.

Privacy Risk: Possibility that the PII of an unrelated individual (who is not under suspicion or the subject of investigation) is collected as part of an incident or investigation about someone else and be unaware of and/or unable to consent to DEA's collection of their PII.

Mitigation: This risk is partially mitigated. By the nature of its operation, the RAVANS tool will likely collect a wide range of communications with the subject (or consensual user), even those from individuals unrelated to any criminal act or investigation. However, RAVANS data undergoes a responsiveness review to identify the information that is responsive to the legal process. The data that is not responsive is marked and siloed from view from the investigative team.

Privacy Risk: A risk exists that members of the public subject to legal process for collection of their information are not aware of that DEA is using RAVANS to collect their information.

Mitigation: This risk cannot be mitigated. In most cases, opportunities to refuse consent may be limited or nonexistent because of the DEA law enforcement purposes for which the information is collected. In the context of an ongoing law enforcement investigation,

providing a suspected violator with notice or the opportunity to consent to the use of his or her information will compromise the ability of law enforcement agencies to effectively enforce the law, and could put law enforcement officers at risk. For this reason, notice of collection and the opportunity to consent to specific uses of the data available through systems like RAVANS are generally not provided.

DEA is publishing this PIA to provide general notice to the public about the data it collects via RAVANS. DEA also provides a very general notice in the applicable SORNs. Further, all data collected by RAVANS is obtained for law enforcement purposes in the course of active investigations. Therefore, the notice requirement is exempted by 28 C.F.R. § 16.98 to the extent RAVANS data becomes part of the DEA's Investigative Reporting and Filing System, particularly with respect to targets of criminal investigations.

Further, the collection of electronic search warrant data is obtained through authorized legal process. The data is used in criminal investigations where the federal rules of criminal procedure are adhered to and require that a defendant be provided a copy of the evidence that will be used in a court proceeding against them and items that are material to the defense. The prosecuting attorney will coordinate with the investigating agent to provide a copy of the intercepted communications and associated metadata to the defendant's legal counsel. This process is known as discovery.

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

Privacy Risk: Potential for use of PII in a manner incompatible/inconsistent with the intended uses of or specified purposes for collection of the information.

Mitigation: This risk is mitigated. Most RAVANS data is obtained through applicable legal process that authorize the data collection and require that the data will be used in furtherance of the relevant criminal investigation for which the data is sought and not for any other purpose. This is accomplished by limiting access to the data to the investigative case team; these individuals annual complete training about safeguarding data. Failure to properly safeguard data could result in disciplinary action. In rare instances, the information is obtained through consent from the owner of the data and is also used in furtherance of the criminal investigation.

Privacy Risk: Potential for a system breach by physical intrusion or technical exploitation of the data at rest or in transit.

Mitigation: This risk is mitigated. DEA uses Security in Depth relying on multiple layers of physical and electronic protection of the system and the data contained within the system. Physical intrusions by unauthorized individuals into DEA facilities are prevented by perimeter security protections such as armed guards and video surveillance (where applicable), and physical access is only possible through controlled entry to all DEA occupied buildings and facilities with PIV card readers for all entries. RAVANS is

housed in a DEA controlled facility that utilizes physical access control measures to prevent unauthorized access. Further, system users must employ multi-factor authentication to access their allowed data sets. The RAVANS data at rest and in transit is encrypted in order to mask the content from unauthorized parties. Protection of information system resources is provided by management, operational, and technical security controls. Access to all records is controlled and limited to approved personnel with an official need for access to perform their duties.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data.

Mitigation: This risk is mitigated. Data in RAVANS itself is deleted two years after the close of the case in accordance with DFN 601-38a2. As a duplicate of information contained in the casefile, deletion from RAVANS, however, does not equate to deletion from the casefile. RAVANS data downloaded to the case file will be deleted from the case file system after the investigative casefile is closed plus 25 years in accordance with DFN 601-39c1. Investigative casefiles are required to be closed in a timely manner and the process is outlined in the DEA agent's manual. The evidentiary copies of collected data are disposed of and their disposition is documented on a DEA Form 48a, which is retained within the investigative casefile. . .

c. Potential Threats Related to the Dissemination of Information

Privacy Risk: Potential for DEA personnel to access the information with no need to know, or to disclose PII to an inappropriate party or for an improper purpose.

Mitigation: These risks are mitigated. Lawfully collected data is logically protected from unauthorized viewing and copying by computer login restrictions that permit only authorized users to access the data. An authorized user's access is limited, controlled and tracked by the system. Specific permission-based restrictions exist at both the application interfaces and the file level. The system is accessed by users with unique and attributable accounts within government facilities. The system is remotely accessed by a limited number of system administrators via a VPN connection and a two-factor authentication process. Separate investigative data sets are only viewable by the authorized members of the investigative team or for prosecution purposes and use of the data is appropriately limited to law enforcement data only. Further, an access request form filled must be filled out for each case and only authorizes the user for that particular case during that time. Each request requires supervisory approval and oversight.

Further, each user annually is required to review and acknowledge the DEA IT Rules of Behavior as part of the mandated online IT Security Training. These individuals confirm they have read and accepted the IT Rules of Behavior for General and Privilege Users regarding the proper handling of all DEA documents and data. The limited distribution of the information from the applications, continual monitoring of access to the applications, and the observance of the IT Rules of Behavior helps mitigate the risk of unauthorized use or disclosure of DEA's pertinent information. For any distribution outside of DEA within the Federal Government, these users must also comply with

similar computer security requirements, participate in annual security training, and acknowledge similar rules of behavior. If users fail to comply with the rules of behavior upon which they have been trained, they are subject to discipline as appropriate up to and including dismissal.