Drug Enforcement Administration

Privacy Impact Assessment
for
Relativity

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 20, 2024

(May 2022 DOJ PIA Template)

[THIS PAGE PURPOSELY LEFT BLANK]

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.)

Relativity, a subsystem of the Drug Enforcement Administration (DEA's) Firebird network, is designed for legal staff within DEA to securely view, process, analyze and report upon data related to legal case work, including document scanning, sorting, and metadata tagging, threading and reporting. The Relativity server footprint consists of 58 servers, of which 40 have Relativity installed and the remainder are file servers containing case data repositories or Analyst servers used to process data in, out, transform, or troubleshoot data associated with various eDiscovery (i.e., electronic discovery) or forensic workflows.

Relativity is used to organize and review unstructured data provided by other DEA IT systems or opposing counsel. Relativity retrieves information by performing a query against the stored data in the Structured Query Language (SQL) database. The database then returns the data in a structured form to the user. Data at rest and transit is encrypted.

DEA has prepared a Privacy Impact Assessment because Relativity is an IT system or project that collects, maintains or disseminates information in identifiable form from or about members of the public.

Section 2: Purpose and Use of the Information Technology

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

The purpose of the Relativity review system is designed for DEA legal staff and investigative personnel to securely view, process, and analyze unstructured data in case-specific workspaces with specific case number/unique identifiers and facilitates the production and/or reporting information of data related to a case. This includes electronic document ingestion, filtering, sorting, tagging, email threading, reporting, and production of respondent data. The case data leveraged by the Relativity system is owned by DEA and exists within the Firebird information system. This leveraged information includes e-mail to and from DEA employees and contractors[1], opposing parties, and third parties as it relates to litigation. The data within Relativity is collected for civil and criminal cases; Freedom of Information Act (FOIA) requests; Equal Employment Opportunity Commission (EEOC) and Merit System Protection

[1] For purposes of this document, "contractors" includes DEA Task Force Officers and Detailees.

Board (MSPB) matters; and internal investigations as authorized by the DEA Office of Chief Counsel.

The Relativity review system enables case team members to search and reduce the overall data down to just that which is responsive to a given matter, often from millions of records to several thousand, greatly reducing review times and thereby conserving valuable agent and/or Office of Chief Counsel resources.

Access to Relativity is limited to approved end users (e.g. legal and investigative personnel), the DEA Digital Evidence Laboratory, and a Relativity Subject Matter Expert (SME) System Administrator. End users are primarily attorneys in the Office of Chief Counsel and staff in its Litigation Support Section. Other personnel authorized by DEA Office of Chief Counsel to access Relativity are paraprofessionals, case agents, US Attorneys or their assigns, and DEA eDiscovery Unit personnel. There are no external users to the DOJ who can access DEA's instance of Relativity. Access to individual electronic case files stored within Relativity will be limited to those authorized end users who have a need to access specific electronic case files and authorized laboratory personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file.

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
X	Statute		21 U.S.C. § 801 et seq.;
	Executive Order		
X	Federal Regulation		28 C.F.R. §§ 0.100 and 0.101; Federal Rules of Criminal Procedure, Rule 16; Federal Rules of Civil Procedure Rule 26
	Agreement, memorandum of understanding, or other documented arrangement		
	Other (summarize and provide copy of relevant portion)		

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. 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	System contains name of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Date of birth or age	X	A, B, C and D	System contains birthdays/ages of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Place of birth		A, B, C and D	System contains places of birth of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Gender	X	A, B, C, and D	System contains genders of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Race, ethnicity or citizenship	X	A, B, C, and D	System contains information about the race, ethnicity and/or citizenship of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Religion	X	A, B, C, and, D	System may contain religion information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	System contains Social Security Numbers of employees, contractors, detailees other federal government personnel, and/or members of the public (US or non-USPERs).
Tax Identification Number (TIN)	X	A, B, C, and D	System contains TIN of employees, contractors, detailees, other federal government personnel, and/or 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
Driver's license	X	A, B, C, and D	System contains driver's license information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Alien registration number	X	A, B, C, and D	System contains alien registration number information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Passport number	X	A, B, C, and D	System contains passport information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Mother's maiden name	X	A, B, C, and D	System contains information on the mother's maiden name of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Vehicle identifiers	X	A, B, C, and D	System contains vehicle identification information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Personal mailing address	X	A, B, C, and D	System contains personal address information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Personal e-mail address	X	A, B, C, and D	System contains email address information of employees, contractors, detailees, other federal government personnel, and/or 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
Personal phone number	X	A, B, C, and D	System contains personal phone number information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Medical records number	X	A, B, C, and D	System may contain medical records number information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Medical notes or other medical or health information	X	A, B, C, and D	System may contain medical information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Financial account information	X	A, B, C, and D	System may contain financial account information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Applicant information	X	A, B, C, and D	System may contain applicant information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Education records	X	A, B, C, and D	System may contain education record information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Military status or other information	X	A, B, C, and D	System contains military information of employees, contractors, detailees, other federal government personnel, and/or 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
Employment status, history, or similar information	X	A, B, C, and D	System contains employment history information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, and D	System may contain employment performance information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Certificates	X	A, B, C, and D	System may contain certificate information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Legal documents	X	A, B, C, and D	System contains legal documents relevant to employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Device identifiers, e.g., mobile devices	X	A, B, C, and D	System may contain device identifier information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Web uniform resource locator(s)	X	A, B, C, and D	System contains Web URL information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Foreign activities	X	A, B, C, and D	System may contain foreign activity information of employees, contractors, detailees, other federal government personnel, and/or 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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, and D	System contains criminal record information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Juvenile criminal records information	X	A, B, C, and D	System may contain juvenile criminal records information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, and D	System contains civil law enforcement information regarding employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, and D	System may contain whistleblower information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Grand jury information	X	A, B, C, and D	System contains grand jury information of employees, contractors, detailees, other federal government personnel, and/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, and D	System contains witness information relevant to employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Procurement/contracting records	X	A, B, C, and D	System may contain contracting information relevant to employees, contractors, detailees, other federal government personnel, and/or 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
Proprietary or business information	X	A, B, C, and D	System may contain business information related to employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, and D	System contains location/tracking information of related to eDiscovery employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, and D	System contains photographic information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
- **Video containing biometric data**	X	A, B, C, and D	System may contain video information of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
- **Fingerprints**	X	A, B, C, and D	System contains fingerprint records of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	X	A, B, C, and D	System may contain voice recordings of employees, contractors, detailees, other federal government personnel, and/or members of the public (US or non-USPERs).
- **Scars, marks, tattoos**	X	A, B, C, and D	System may contain scar or other bodily marks information of employees, contractors, detailees, other federal government personnel, and/or 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
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **8DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	**A** and B	Audit system retains the User ID data of employees, contractors, detailees, and other federal government personnel.
- **User passwords/codes**			
- **IP address**	X	A and B	Audit system retains the IP address data of employees, contractors, detailees, and other federal government personnel.
- **Date/time of access**	X	A and B	Audit system retains access data of employees, contractors, detailees, and other federal government personnel.
- **Queries run**	X	A and B	Audit system retains the queries of employees, contractors, detailees, and other federal government personnel.
- **Content of files accessed/reviewed**	X	A and B	Audit system retains information about the content of viewed files by employees, contractors, detailees, and other federal government personnel.
- **Contents of files**	X	A and B	Audit system may retain information about the content of viewed files by employees, contractors, detailees, and other federal government personnel.
Other types (please list all other types of identifying information collected and describe as completely as possible):	X	A, B, C, and D	Due to the nature of e-discovery data collection and processing, various types of PII will potentially be a part of gathered evidence in support of legal investigations.

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	

Phone	X	Email	X		
Other (specify): As collected by the Cybersecurity Operations, Response, and Engineering Unit (TCVV) under the authorization of the Office of Chief Counsel, email as well as profile data ("profile data" being defined as including but not limited to a DEA user's computer desktop, various system, and My Documents folders, as well as data identified in, but not limited to shared network folders, and scanned data collected as part of the information gathering process). Information is collected directly from DEA users during FOIA, EEOC, and MSPB matters. Information concerning subjects of investigation, criminal matters are collected from source systems.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal entities	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer).	X	MLAT agreements between foreign countries and the United States.	
Other (specify): Mutual Legal Assistance Treaty (MLAT) agreements between foreign law enforcement agencies and the United States allow for collection of data or evidence from foreign law enforcement agencies.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
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		X	Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to

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.**
				further stated lawful investigations both domestic and international.
DOJ Components	X		X	Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international.
Federal entities	X			Data is disseminated case by case to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international.
State, local, tribal gov't entities	X			Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international. There is no direct login access to this data, which is provided out to the requesting party as authorized by law and Memorandum of Agreement or Understanding.
Public	X			Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international. There is no direct login access to this data, which is provided out to the requesting party as authorized by law.

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 disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international. There is no direct login access to this data but is provided out to the requesting party as authorized by law.
Private sector	X			Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international. There is no direct login access to this data, which is provided out to the requesting party as authorized by law.
Foreign governments	X			Data is disseminated to respondents in response to legal requests for data, including criminal, civil, and administrative discovery as well as for internal investigations or to further stated lawful investigations both domestic and international. There is no direct login access to this data, which is provided out to the requesting party as authorized by law and MLAT where applicable.
Foreign entities	X			Case-by-case basis, in which the specific method depends upon the nature of the matter and the country involved.
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.

Not applicable.

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.

Because Relativity handles discovery for almost all criminal and civil cases facing DEA, multiple SORNS may apply to parts of the system and provide general notice:

- JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012);
- JUSTICE/DEA-011, Operations Files, 52 Fed. Reg 47182 (Dec. 11, 1987);
- JUSTICE/DEA-INS-111, Automated Intelligence Records System (Pathfinder), 55 Fed. Reg. 49146 (Nov. 26, 1990);
- JUSTICE/DEA-022, El Paso Intelligence Center (EPIC) Seizure System (ESS), 71 Fed. Reg. 36362 (June 26, 2006);
- JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 04, 2001);
- JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26580 (May 4, 2012);
- JUSTICE/DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sep. 24, 2002);
- JUSTICE/DOJ-008, Department of Justice Grievance Records, 68 Fed. Reg. 61696 (Oct. 29, 2003)
- JUSTICE/DOJ-017, Department of Justice Giglio Information Files, 80 Fed. Reg. 16025 (Mar. 26, 2015);
- OPM/GOVT-3 Record of Adverse Actions, Performance Based Reduction In Grade and Removal Actions, and Termination of Probationers, 71 Fed. Reg. 35350 (June 19, 2006).

Production and dissemination of discovery is made in response to lawful requests for data or discovery obligations in, but not limited to: lawsuits, investigations, or attorney-supervised activities, such as preparation for internal misconduct reviews and FOIA productions. These disclosures are therefore the responsibility of the DEA Office of Chief Counsel. In many cases, disclosures are never revealed to the person named in the records, as they may never be made aware their data was collected, reviewed, disclosed and/or produced. In many instances, information covered by DEA investigative SORNs are exempt from the notice requirements of the Privacy Act as notifying a subject of an investigation may have an adverse impact on the investigative activity.

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.

DEA employees and contractors are required to provide certain information including their name and address and receive notice when using government issued cell phones and computers that they have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system and that, at any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system. However, DEA employees are not required to provide other personal information that they might choose to put in government communications.

Regarding criminal investigations, a person who is cooperating with law enforcement may choose to allow their data to be collected as evidence. This process is referred to as a consent. Persons who are the implicated in investigations and whose personal information are collected during a criminal investigation (e.g., through seizure pursuant to a search warrant) do not have an opportunity to decline the collection, use, or dissemination of information in Relativity. Notification beforehand cannot be afforded to a subject of an active investigation due to the risk of compromising the integrity of the investigation. 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.

Data is collected for criminal and civil investigative purposes and can be provided as part of criminal or civil discovery. Individuals can request system information via the Freedom of Information Act (FOIA) or Privacy Act (PA) but such information would likely be subject to a FOIA or PA exemption. Individuals may submit a FOIA or PA request at https://www.dea.gov/foia.

Section 6: Maintenance of Privacy and Security Controls.

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls.** **Provide date of most recent Authorization to Operate (ATO):** Relativity is in ongoing authorization. The ongoing authorization request was approved on 2/8/2024. **If an ATO has not been completed, but is underway, provide status or expected completion date:**
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:** The only POA&M Relativity has that pertains to privacy controls is approving this document. Once this document is approved, the PO&AM will be closed.
	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.** Relativity was assigned security category of High as defined in FIPS-199 based on the aggregation of the information of several different and seemingly innocuous types of information (e.g. social security numbers, first/last name, birth dates and home address) and Criminal Investigation and Surveillance together reveals sensitive information.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** DEA monitors 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 affect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO, 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:** The application audit logs are reviewed daily as part of the TCVV review process. The audit logs are reviewed based off alerting received from monitoring applications which occur when an alert is activated. Operations & Response team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts. DEACORE reviews alerts received from monitoring applications that feeds into the log management tool and contact the system owner. Additionally, the program management office performs periodic reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws. The system owner is responsible for complying with all guidelines, policies, and laws. The ISSO for Relativity is responsible for validating that users comply with said governance while TCVV enforces actions based upon an infraction (cybersecurity incidents, policy violations). TCVV perform validation for compliance to governance during risk assessments which are scheduled (ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation.
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**. Yes, as a standard operating procedure, all DEA contracts provide that contractors are bound by the Privacy Act, other applicable laws and DEA and 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:** Security training is conducted annually and throughout the year in order to provide an overview of agency employees' obligations to protect PII. The component has a requirement for all employees, to include contract employees, to complete the mandated Cyber Security Awareness Training annually.

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?

Key Physical Controls: Physical and Environmental controls are enforced across all DOJ's buildings as part of its common control requirements. This is enforced with defense in depth.[2] All DEA buildings are guarded by security personnel at the entrance of the office. In addition, employees are required to authenticated with their Personal Identity Verification card (PIV)[3] before being granted access to the building. Access to Relativity system is based on need to know which requires authentication via the PIV card as well.

Key technical controls for relativity data in transit and at rest: Access to all Relativity electronic records is controlled. Security controls such as access controls and the National Institutes of Standards and Technology (NIST) 800-53 Rev. 5 Identification and Authentication control family are utilized in Relativity.[4] Users access to Relativity must electronically be verified and accepted in the form of a username on the Firebird network and adequate permissions to view the data. This is limited by group policy to few personnel and is designed to avoid unauthorized access to Relativity data at rest.

The system is accessible on the DEA Firebird network and ensures security and fidelity of a user's account through additional means of verification, as enforced by PIV system. Access to Relativity is limited to approved end users (e.g. paraprofessionals, GS-1811 agents, staff from DEA's Office of Chief Counsel, etc.), the DEA Digital Evidence Laboratory, and a Relativity Subject Matter Expert (SME) System Administrator. Operations and management of the Firebird infrastructure is performed by DEA's Enterprise Operations Management Unit, (EOMU) who will have full administrative access to administrative levels of data, such as SQL, but do not have the ability to interact with Relativity workspace content.

Relativity is part of the Stratus cloud environment.[5] Stratus has all data at rest and in transit encrypted.

---

[2] Defense in depth refers to an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. See https://csrc.nist.gov/glossary/term/defense_in_depth.

[3] A PIV card is a physical artifact (e.g., identity card, "smart" card) issued to a government individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable). PIV requirements are defined in FIPS PUB 201. *See* https://csrc.nist.gov/glossary/term/personal_identity_verification.

[4] *See* https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

[5] Stratus is covered by separate privacy documentation.

Key Administrative Controls: The Relativity application can only be accessed by users who are granted permissions to Relativity. Access to Relativity is limited to a small group of users approved by DEA supervisory attorneys. DEA supervisory attorneys will submit an access request (via e-mail) to the Relativity SME System Administrator, and their designees for a given matter. Data will be populated to the matter and the users are granted access. Office of Chief Counsel eLitigation team members and/or the Relativity SME provides training to ensure all users are adequately skilled to operate the application. In addition, the system was designed to "silo" or isolate data by investigative case. It is impossible to search or review data across multiple cases at the same time.

In addition, all laboratory staff are required to attend training prior to being granted access to Relativity as provided by the Digital Evidence Lab (SFL9). Each user must also complete the Cybersecurity Awareness Training and Records and Information Management training annually. DEA follows the guidance set forth by DOJ Security Standard policy and procedure. The security assessments and authorizations for Certification and Accreditation adhere to DOJ standards.

Further, all DEA employees and federal contractors agree to and certify to the DEA Standards of Conduct on an annual basis. Access to the system itself is protected by authentication controls, role-based access controls, and system auditing. Access to the building where the system is housed is protected by physical building security, including security guards, access badges, and security cameras. Administrative access to individual electronic case files stored within Relativity will be limited to those authorized laboratory personnel who manage and have direct control over case file information, including their supervisors who have a legitimate need to review the file. To further prevent unauthorized use by employees, audit logs are kept and are available for review. When there is an alert, the system owner is notified, and an investigation and/or corrective action is taken.

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.)

DEA follows the eDiscovery Unit Records Management Policy which describes in detail the length of time data must be retained in accordance with the DEA Records and Information Management (RIM) data retention policies. In general, documents that are collected are retained until the matter reaches final disposition and after which are retained as the RIM dictates for the type of matter that the data was collected for. For example, data from a FOIA request has a separate retention timeframe post-disposition than data from a criminal case, and data for each is kept in accordance with the appropriate RIM guidance for the time to final disposition.

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:

Due to the expansive range of legal matters and evidence in support thereof that may be covered by the systems, multiple SORNS are or may be applicable:

- JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012);
- JUSTICE/DEA-010, Planning and Inspection Division Records, 52 Fed. Reg. 47182, 213 (Dec. 11, 1987);
- JUSTICE/DEA-011, Operations Files, 52 Fed. Reg. 47182, 214 (Dec. 11, 1987);
- JUSTICE/DEA-012, Registration Status-Investigation Records, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987);
- JUSTICE/DEA-013, Security Files, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987);
- JUSTICE/DEA-022, El Paso Intelligence Center (EPIC) Seizure System (ESS), 71 Fed. Reg. 36362 (June 26, 2006);
- JUSTICE/DEA-INS-111, Automated Intelligence Records System (Pathfinder), 55 Fed. Reg. 49146, 182 (Nov. 26, 1990)
- JUSTICE/DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (June 04, 2001);
- JUSTICE/DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, 77 Fed. Reg. 26580 (May, 4, 2012);
- JUSTICE/DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sep. 24, 2002);
- JUSTICE/DOJ-008, Department of Justice Grievance Records, 68 Fed. Reg. 61696 (Oct. 29, 2003);
- JUSTICE/DOJ-017, Department of Justice Giglio Information Files, 80 Fed. Reg. 16025 (Mar. 26, 2015);
- OPM/GOVT-1, General Personnel Records, 77 Fed. Reg. 79694 (Dec. 11, 2012);

- OPM/GOVT-2, Employee Performance File System Records, 71 Fed. Reg. 35347 (June 19, 2006);
- OPM/GOVT-3, Record of Adverse Actions, Performance Based Reductions In Grade and Removal Actions, and Termination of Probationers, 71 Fed. Reg. 35350 (June 19, 2006).

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 the 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. Data is collected for the Relativity review system from DEA custodians, information about suspects or from suspects in criminal investigations, and ancillary communications and data which is present in the collected data from other custodians. Relativity is only gathering information that has already been collected by other DEA systems, and only is gathered and accessed in Relativity for the limited purpose of securely viewing, processing, analyzing and reporting upon data related to legal case work. To the extent that any over collection has occurred, it was done so by other systems outside the scope of Relativity's purpose. However, collection of data for input into Relativity is limited to that data DEA custodians assess as relevant to the specific civil or criminal matter for which it is being collected.

Privacy Risk: Chance that some PII collected will not be directly relevant and necessary for DEA to accomplish its purpose or mission, such as belonging to an unrelated individual not under suspicion.

Mitigation: This risk is partially mitigated. As noted above, Relativity is only gathering information that has already been collected by other DEA systems and only for the limited purpose of securely viewing, processing, analyzing and reporting upon data related to legal case work.. To the extent that the PII previously collected appears not to be necessary or is irrelevant to a DEA investigation, the collection determination made was outside the scope of Relativity's purposes. Generally, the following measures help ensure that evidence collected is both relevant and necessary for the investigation: (1) extensive training on the proper collection of relevant evidence given to criminal investigators; (2) investigative procedures and policies detailing the proper collection of evidence; and (3) supervisory involvement in all aspects of the investigation, including collection of evidence. If evidence collected is found not to be relevant, such evidence will be marked as not relevant and/or segregated from the relevant evidence.

Additionally, relevance is reassessed before being input into Relativity. Attorneys supervising

cases decide what types of categories of documents within other DEA systems would be responsive and which custodians might have responsive documents. Only these documents and data are then placed in Relativity for a given case. Although DEA personnel use search terms and enterprise-level applications to search other DEA systems to identify possibly responsive materials to ingest into Relativity for case teams to review, the data that is segregated out as outside the scope and not responsive is generally not separately manually reviewed.

Privacy Risk: A risk exists that members of the public subject to certain court orders or administrative subpoenas are not given specific notice their information is being collected.

Mitigation: This risk cannot be fully mitigated. Although the decision for DEA to collect any individual's PII are made by users of systems other than Relativity, providing notice in law enforcement investigations is often inherently limited. In most cases, opportunities to refuse consent may be 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 would 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 Relativity are generally not provided.

However, when information is collected via search warrants or other legal process, the subjects of the collection generally receive notice of the collection, absent a non-disclosure order. DEA also provides a very general notice in the applicable SORNs for the various investigation and intelligence systems of records into which newly collected PII would first be placed. Moreover, DEA is publishing this PIA to provide general notice to the public about the data it maintains within Relativity.

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

Privacy Risk: The system's administrative controls may be insufficient to prevent unauthorized individuals within DEA or DOJ from accessing the system's PII without a need to know or using the information for a purpose or in a manner unrelated to the reason why the information was collected (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. Relativity has robust access controls. Not every DEA employee can access Relativity. Users are primarily attorneys in the Office of Chief Counsel and staff in its Litigation Support Section. Other personnel authorized by DEA Office of Chief Counsel to access Relativity are paraprofessionals, case agents, US Attorneys or their assigns, and DEA eDiscovery Unit personnel. There are no external users to the DOJ who can access DEA's instance of Relativity. Actions by administrative users, who are part of the eDiscovery Unit staff, are recorded by a monitoring application when they are logged on. The monitoring application is monitored by the Department of Justice.

Additionally, Relativity users are granted access to only workspaces which have been approved by Office of Chief Counsel or at their direction. The users cannot access either the raw data or content of workspaces they do not have access to. Relativity administrative staff at SFL9 are the only personnel who have full access to workspaces and raw data. TCVV, who collect the data, have access to the raw data which they collect and deposit into the Relativity file servers as part of their process. The network team that maintains the servers on which Relativity resides have access to the raw data as well as the SQL databases where Relativity's data resides, but cannot access the Relativity review system.

Furthermore, all user activities are logged in Relativity and audit logs are reviewed daily as part of the TCVV review process. The audit logs are reviewed based off alerting received from monitoring applications which occur when an alert is activated. Attorneys and staff also receive training on the handling of PII. All personnel are permitted to access only the workspaces for which they have been granted access, with the exception of eDiscovery Unit personnel, who have complete access to all workspaces and data. eDiscovery Unit personnel, and other administrative users, receive greater security scrutiny than regular users. For example, all actions performed by eDiscovery Unit staff when logged onto the servers are recorded by the monitoring application (covered by separate privacy documentation) and monitored by DOJ Office of the Chief Information Officer.

Privacy Risk: DEA personnel may mishandle or fail to safeguard PII without sufficient privacy and security controls for handling and protecting PII.

Mitigation: This risk is mitigated, primarily with the physical, technical, and administrative privacy and security controls referenced in Section 6.2 above.

In addition, the data collected in Relativity has been authorized by courts of relevant jurisdiction or by DEA policy. Whenever possible, protective orders are entered into which protect sensitive data such as PII, and sensitive data is reviewed by attorneys from the DEA Office of Chief Counsel as to whether redaction or otherwise withholding is necessary to protect custodial information.

Even where attorneys request that data be added to Relativity outside litigation where no protective orders are available, such as review for responses to FOIA requests, or for internal investigations, the attorneys and staff reviewing documents will determine if sensitive data should be redacted or withheld before further use. Withheld documents may contain attorney client privileged, law enforcement sensitive, or other lawfully privileged categories of data.

Privacy Risk: PII may be accessed and altered impermissibly, thereby affecting the accuracy and reliability of the information.

Mitigation: This risk is mitigated. Data within the Relativity review system cannot be altered without significant effort, or by downloading the data and manually changing it. As the system is designed for review, it is designed for presentation but not alteration of data. There is always the risk that an attorney or support staff could download PII and use it for impermissible activities, but the risk is low, as the reviewers are licensed attorneys who adhere to a strict set of legal ethics, and their support staff.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Potential for DEA personnel to share or disclose PII Information to an inappropriate third party.

Mitigation: This risk is partially mitigated. The primary purpose of Relativity is to permit attorneys and their staff to review DEA files for relevant documents that will be produced though discovery to opposing counsel or to employees in criminal prosecutions, civil litigation and administrative hearings. In rare instances, Relativity is used by the Office of Chief Counsel to review discovery records obtained from opposing parties. Therefore, the disclosure of PII information is an inherent outcome in most Relativity use and is governed by DOJ and DEA discovery policies, DEA Privacy protection policies, and judicial oversight in litigation matters.

In fact, whenever possible, protective orders are entered into which protect sensitive data such as PII, and potentially sensitive disclosures are reviewed by DEA attorneys as to whether redaction or withholding is necessary to protect information. As this data is reviewed by attorneys in their capacity as officers of the court of relevant jurisdiction, it is incumbent on the attorney(s) to ensure that adequate safeguards are employed when collecting, reviewing, and producing data.

Further, data is often transferred to recipients using DOJ's Justice Enterprise File Sharing (JEFS)[6], which is an encrypted File Transfer Protocol (FTP) method to transfer files across the internet. When datasets are very large and exceed the electronic transfer limits of JEFS, data is sometimes placed onto external hard drives and shipped via FedEx or other common carrier to the data recipient. The eDiscovery Unit and the responsible DEA attorney confer prior to any data being released. In the normal course, any data released by DEA is done so in accordance with DEA's IT Rules of Behavior and is secured via encryption and on a DEA approved device. In certain instances, it is determined that encryption is not feasible. For example, very large (multiple terabyte) data transfers are too big for existing DOJ encrypted transfer systems. In a not insignificant number of instances the receiving parties for encrypted discovery do not have the capacity to decrypt the data due to their own technical limitations. In these circumstances, the safest available delivery method is sought, such as in-person pick up of discovery production by the DOJ litigating attorney. In addition, DEA's Digital Evidence Lab seeks appropriate waivers from DEA's Office of the Chief Information Officer to produce unencrypted data.

Where unencrypted hard drives are sent, loss or erroneous receipt by non-parties could result in the compromise of ongoing investigations, and expose the PII of informants, DEA personnel, their families, and even targets of DEA investigations. Encryption of PII over electronic communication is DOJ policy and is the default for delivery of hard drives by common carrier, unless the responsible DEA attorney confirms in writing that an unavoidable

[6] JEFS is covered by separate privacy documentation. See https://www.justice.gov/d9/pages/attachments/2021/09/30/jefs_pia_final_draft_11-30-2017.pdf.

circumstance prevents the use of encryption and sufficient security measures are otherwise taken in light of the sensitivity of the data at issue.

Information within the DEA Relativity data repositories resides in the DEA Firebird Network environment as a tenant with robust access controls that make unintended disclosures unlikely. System information such as SQL tables or access methods are generally not shared with outside parties, except in very limited instances such as upgrades or troubleshooting when necessary.

Further disclosures of DEA documents produced to parties in litigation would, of course, then be beyond the custody and control of the DEA. However, whenever possible, protective orders are entered into which would protect sensitive data such as PII, from further unauthorized disclosures. Moreover, prior to sharing Relativity data with foreign partners, DEA enters into agreements with those partners detailing how that data can and cannot be shared further.