Drug Enforcement Administration

Privacy Impact Assessment
for the
DEA Title 21 Coordination System (DEA T-21)

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

Approved by: Andrew J. McFarland
Senior Counsel
Privacy and Civil Liberties Office
U.S. Department of Justice

Date approved: August 27, 2025

(July 2023 DOJ PIA Template)

Section 1: Executive Summary

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

The purpose of the Drug Enforcement Administration (DEA) Title 21 Coordination System (DEA T-21) is to notify DEA that Homeland Security Investigations (HSI) (an investigative division within the Immigration and Customs Enforcement component of the Department of Homeland Security) is conducting an investigation involving violation of Title 21 of the United States Code (specifically § 801 *et seq.* of the Controlled Substances Act)[1] thereby effectuating the core principles of the DEA-HSI Interagency Cooperation Agreement through the coordination and deconfliction of DEA and HSI investigations to ensure officer safety, enhance the impact on drug trafficking organizations, eliminate duplication of DEA effort, and ensure DEA and HSI work together to reduce the availability of drugs in the United States.

The DEA T-21 system has DEA and HSI personnel entering drug-related investigation information into a dedicated website to populate a centralized database that collects and shares their information across the two agencies to assist the agencies to deconflict their Title 21 cases.

DEA T-21 users obtain access from a DEA T-21 portal on the De-confliction & Information Coordination Endeavor (DICE 2.0) external-facing website, which itself is resident on the external facing portion of the DEA CONCORDE[2] General Support System. Only HSI and DEA personnel, not all DICE 2.0 users, will have access to the DEA T-21 website.

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.

Use of DEA T-21 will replace the current use of emails to support the core principles of the DEA/HSI Interagency Cooperation Agreement. The DEA T-21 application will be used by HSI and DEA agents to replace legacy communication channels. DEA T-21 will involve DEA and HSI personnel entering drug-related investigation information into a dedicated website to populate a centralized database that

---

[1] The Controlled Substances Act, 21 U.S.C. §§ 873(b) and 878, authorizes the Attorney General to designate Homeland Security Investigations special agents, regardless of whether their duties ordinarily include Controlled Substances Act (CSA) investigations, as well as state and local law enforcement officers serving on HSI task forces, to investigate drug offenses ordinarily within the Drug Enforcement Administration's sole jurisdiction. When investigating drug offenses pursuant to such designations, all HSI personnel must operate under DEA's supervision.

[2] CONCORDE is covered by separate privacy documentation.

will collect and share information across the two agencies to assist deconfliction on HSI or DEA Title 21 cases.

The DOJ Deconfliction Policy defines deconfliction as, "The sharing of limited investigative information between federal, state, local, and tribal law enforcement entities in order to identify targets of common investigative interest and activities." Once the common link is identified; agents, deputies, and officers are notified and provided contact information to share and coordinate information in order to avoid conflicting or competing equities and to synchronize investigative activities. Generically, there are three different types of deconfliction. The three types are defined as follows:

- **Investigative data deconfliction**: is the deconfliction of significant investigative information, including but not limited to, telephone numbers, push-to-talk numbers, e-mail addresses, Internet Protocol addresses, Blackberry PINs, Mobile Earth Station IDs (MES IDs), Registrant IDs, aircraft tail numbers, Financial Account Numbers, Vehicle Identification Numbers (VINs), and License Plate Numbers.

- **Target deconfliction**: is the deconfliction of significant investigative information (target name, date of birth, and sex) that pertains to active investigative targets.

- **Event deconfliction**: is the deconfliction of significant investigative information that relates to significant occurrences, or anticipated occurrences, such as search warrants, arrest warrants, surveillances, buy-busts, and enforcement operations, to include undercover purchases of evidence, arrests, etc. Significant investigative information, for purposes of this document, is information developed or identified through an approved and active criminal investigation.

DEA achieves its deconfliction services through separate but related information systems: internally, DEA uses an internal system called the DEA Analysis and Response Tracking System (known as DARTS 2.0), and external law enforcement agencies can deconflict with DEA investigations through the DEA's De-Confliction Information Coordination Endeavor (known as DICE 2.0)[3], which leverages the DEA CONCORDE General Support System backend infrastructure. HSI can deconflict with DEA investigations through the DEA T-21 web application, which is accessed through the DICE 2.0 system. HSI personnel can only enter information into the DEA T-21 web application interface and will only be able to view matching data pulled from the DICE 2.0 databases. However, DARTS and DICE offer only investigative data and target deconfliction searching, not event deconfliction. As such, DEA T-21 assists HSI with only Target and Investigative deconfliction.

As noted, DEA T-21 users access the DEA T-21 portal on the DICE 2.0 external-facing website, therefore, the actual deconfliction processing is done in DICE 2.0, but verified in DEA T-21. The types of information HSI personnel enter into T-21 and can view in T-21 for deconfliction using DICE 2.0 are as follows:

---

[3] DARTS and DICE are covered under separate privacy documentation. See DEA Analysis and Response Tracking System 2.0-Deconfliction Information Coordination Endeavor 2.0 (DICE 2.0-DICE 2.0) PIA at: https://www.dea.gov/foia/privacy-impact-assessment

- Federal Bureau of Investigation Identifications (IDs)
- Electronic mail (Email) address
- Sex
- Phone Numbers
- Names (First, Middle, Last) and other name
- Social Media Moniker/App (IOD) and associated passwords
- Social Security Number (SSN)
- Date and Place of Birth
- Trinity Check ID

When a search is conducted by HSI users using DICE 2.0, HSI users must have the following: Phone Number, Trinity Check Id and Case number to submit a DEA T-21 investigation. If the HSI users do not have all the correct information to submit a DEA T-21 coordination request, when it is validated against DICE 2.0, an error will appear within DEA T-21. The HSI user will run a deconfliction in DICE 2.0 on the phone number. The T21 Coordination system will validate the case number, phone number and deconfliction trinity check ID matches that are within the last 30 days, before allowing a HSI user to submit an investigation. HSI users will not be able to download or export any results the system returns. If there is no DEA investigation, the system will so indicate and state a deconfliction was completed within the last 30 days.

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 Controlled Substances Act, 21 U.S.C. § 801 et seq.; Reorganization Plan No 2. of 1973, 87 Stat. 1091 (1973), reprinted as amended in Pub. L. 93–253, § 1 (1974)
Executive Order	Executive Order No. 11727,
Federal Regulation	38 Fed. Reg. 18357 (July 6, 1973)
Agreement, memorandum of understanding, or other documented arrangement	Interagency Cooperation Agreement between the U.S. Drug Enforcement Administration (DEA) and U.S. Immigration and Customs Enforcement (ICE) Regarding Investigative Functions Related to the Controlled Substances Act (June 18, 2009), as amended by Joint Letter on the DEA-ICE Interagency Cooperation Agreement (January 5, 2021)
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	Name of case agent and target of investigation of other federal Government personnel and members of the public (US and non-USPERs)
Date of birth or age	X	C and D	Date of birth and age for members of the public (US and non-USPERs)
Place of birth	X	C and D	Place of birth for members of the public (US and non-USPERs)
Sex	X	C and D	Sex for members of the public (US and non-USPERs)
Race, ethnicity, or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Collect full and disseminate truncated for members of the public (US and non-USPERs)
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number	X	A, B, C and D	Personal Phone numbers of members of the public (US or non-USPERs) collected/disseminated; identities of DEA and other government personal may also be included.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other 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
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Only the FBI Number, where applicable, is collected for members of the public (US and non-USPERs)
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			

(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
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	System UserID collected of employees, contractors, local, state, tribal, and other federal government personnel
- **User passwords/codes**		A and B	User passwords/codes and related information collected of employees, contractors, and other federal government personnel.
- **IP address**	X	A and B	System IP addresses, and related information collected on employees, contractors, and other federal government personnel.
- **Date/time of access**	X	A and B	System audit log date/time of access and related information collected on employees, contractors, and other federal government personnel.
- **Queries run**	X	A and B	System audit log queries of access can be run and related information collected on employees, contractors, and other federal government personnel
- **Contents of files**			
Other (please list the type of info and describe as completely as possible):	X	C and D	Possible collection/dissemination of Websites Shipping Tracking IDs, Social Network User IDs, Social Media account passwords; Darknet monikers, accounts and passwords; IP addresses used; electronic serial numbers, etc. and other unknown PII affiliated with members of the public (US or non-USPERs). Further, in many cases, gender may be inferred from name information that is kept.

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

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

Other (specify):

Government sources:					
Within the Component	X	Other DOJ Components	X	Other federal entities	X
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): DEA interconnected systems and applications have multiple internal and external data providers that are authorized or have entered into an agreement to send and/or receive the information from authoritative sources prior to transmission to the DICE 2.0 application where the documented deconflicted items for T-21 web application can be provided.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
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	DEA System admin/Auditing data may be used/shared to troubleshoot application issues. Access control data is shared with the DICE 2.0 application within DEA.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
DOJ Components	X			DEA and HSI data information may be shared with other DOJ law enforcement for investigations regarding drug related crimes.
Federal entities	X		X	Case information is shared with HSI for deconfliction, as is the purpose of the system.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
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.

No data from this system is released 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.

There will be no notice provided to individuals informing them of collection as the DEA T-21 application is only accessible to DEA cleared personnel (employee, contractors) at the appropriate classification level, job function, with access credentials, with a need to know have access to DICE 2.0. The system is also accessible to the DEA Office of Information System personnel to perform development and administrative duties but would not be accessible to the members of the public.

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.

There will be no opportunities for individuals to voluntarily participate in the collection of information in the DEA T-21 Application. Since the information inputted and deconflicted within the DEA T-21 application would come from the DEA or HSI T-21 personnel, the individual would have no control or knowledge of what information is added or updated within the DEA T-21 application. Moreover, since the information inputted concerns targets of ongoing criminal investigation, it is not advisable or feasible to give these persons knowledge of their information being inputted into the system.

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.

DEA's public facing website contains a Freedom of Information Act (FOIA) and Privacy Act (PA) webpage which provides members of the public with procedures and 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.

People who are subjects of DEA investigations and who are not prosecuted generally will not gain access to the information in T-21, to include the Concorde hosting platforms pertaining to them. T-21, as part of DEA's Investigative Reporting and Filing System (and other listed systems of records), has been exempted from access and amendment, and correction requirements of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2) (see 28 C.F.R. §16.98). Information in T-21 are also records complied for law enforcement purposes and thus also excluded from production under the Freedom of Information Act (FOIA) because it is compiled for investigative law enforcement purposes. (see 5 U.S.C. §552(b)(7)). Where compliance would not appear to interfere with or adversely affect the law enforcement or counterterrorism purposes of this system, or the overall law enforcement process, the applicable exemption may be waived by the DEA in its sole discretion.

Section 6: Maintenance of Privacy and Security Controls

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

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):**

	The DEA Title 21 ATO leverages the DICE 2.0 ATO, however a separate profile will be maintained in JCAM for the child system. The DICE 2.0 ATO was granted on January 12, 2023, and was extended on February 25, 2025. **If an ATO has not been completed, but is underway, provide status or expected completion date:** The ATO for DEA T-21 was extended on February 25 30, 2025, but will expire and need renewal on March 31, 2026. **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:** N/A
	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:** DEA T-21 was assigned the security category of Medium 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) 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 and updates the information system's security plan and other relevant information system documentation, such as the system privacy plan, as appropriate, throughout the information system's lifecycle. DEA reports changes in the security or privacy status of the system to appropriate officials on a regular basis. Significant changes to the system require reauthorizations by the DEA Authorizing Official. Significant changes that effect the information system's creation, collection, use, processing, storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the CPCLO (Chief Privacy and Civil Liberties Officer), or a duly authorized official, prior to reauthorization by the Authorization Official.

	DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement. DEA's Senior Component Official for Privacy reviews significant changes.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the DEA T-21 information system audit records on a daily and continuous basis for indications of inappropriate or unusual activity in accordance with DEA Incident Response Plan. DEA TCVV monitors DEA T-21 using an event correlation tool to identify and report findings to the ISSO for further investigations upon detection of suspicious activities. Any findings are reported to DOJ Security Operations Center using the Justice Management Division Remedy ticketing system.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. All contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each DEA contract awards (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*). DEA contractors have binding contractual obligations to adhere and comply protecting the organization's information and participates in the DOJ/DEA Annual Cybersecurity Awareness Training (CSAT) requirements to acknowledge Privacy Act requirements in accordance other applicable laws, and as required by DOJ policy. All procurements include standard contract language as part of the DEA Service Acquisition process.
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:** All DEA employees including contractors must conduct both Cyber Security Awareness Training (CSAT) and Privacy Act training during onboarding as a new employee/contractor, then must take a CSAT refresher annually thereafter. Required training is distributed and tracked via the DOJ Learning Management System DEALS. This training is applicable to all DEA component personnel and also covers the DOJ and DEA IT rules of behavior which are re-signed annually. In addition, the Office of Chief Counsel (OCC) is working on a role-based annual privacy training which will be published soon.

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?

Administrative privacy and security controls:

Numerous processes/controls have been implemented by DEA to ensure collected data is required and relevant. The process:

- Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group/shared, service, guest/anonymous, and temporary/emergency accounts;
- Assigns account managers for DEA T-21 accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of DEA T-21 to the application through group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by El Paso Intelligence Center[4] User Access Management (UAM) Team Account Managers for requests to create DEA T-21 accounts.

Through the utilization of Microsoft Active Directory (AD), access to this data is controlled to system administrators and personnel that have a need to know based on their position within the organization. This information is used to create access controls and separation of duty. Further, no unauthorized individuals would be allowed to gain access to information within the DEA T-21 application since the DICE 2.0 application is only accessible by DEA or HSI cleared personnel (employee, contractors) at the appropriate classification level, job function, with access credentials, with a need to know have access to DICE,

Technical privacy and security controls

The security measures for DEA T-21 (and associated DICE/DARTS systems) comprise both multi-layered encryption and continuous network monitoring. Regular security audits are conducted to ensure these systems' defenses remain robust against known and emerging threats. DEA T-21 is an accredited system which are compliant with NIST 800-53 (rev 5) Security and Privacy Controls for Information Systems and Organizations. DEA T-21 and DICE/DARTS follow DOJ and DEA continuous monitoring requirements in order to maintain their Authority to Operate (ATO) approvals. Compliance requirements are tracked via Plan of Action and Milestone (POAMs) within DOJ's Joint Cybersecurity Assessment and Management (JCAM) system portal, which is monitored by DEA leadership, Information System Security Officers, and IT management. The control regime:

- Creates, enables, modifies, disables, and removes information system accounts in accordance with DOJ Order 0904: Cybersecurity Program and applicable information system policy and procedures;
- Monitors the use of information system accounts (e.g. logins, logouts, file access);

[4] For more information on EPIC *see* forthcoming EPIC Inquiry System PIA, *available at https://www.dea.gov/sites/default/files/2018-07/epic_8_4_06.pdf*

- Notifies account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage changes;
- Authorizes access to DEA T-21 based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions;
- Reviews accounts for compliance with account management requirements.
- Creates, enables, modifies, disables, and removes DEA T-21 accounts in accordance with DOJ Order 0904: Cybersecurity Program and applicable information system policy and procedures;

Physical privacy and security controls:

Deconfliction occurs within DICE 2.0, both DICE 2.0 and DEA T-21 are deployed within a DEA secured data center. This data center provides physical protection for all hosted systems to include servers, switches, and other devices employed to support the DEA mission. In addition, the data center supplies electrical and HVAC systems for the hosted components. The data center utilizes numerous safeguards to include guards who monitor the facility. Entry includes two sets of doors, the first utilizes a Personal Identity Verification (PIV) Card which is scanned for entry. The second door requires use of the PIV as well as the associated individual PIN. Cameras have been deployed at critical locations to include entry ways. Metal Detectors have been employed for any visitors that do not have a PIV. All physical controls for DICE 2.0 (and the associated DARTS database) are inherited from the data center.

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.)

The information transmitted through DARTS 2.0 and DICE 2.0 to the T-21 web application will be retained for at least 90 days to accomplish the intended purpose of the sharing and will be retained only in accordance with DOJ and DEA Records Management Policy and Procedures derived from the National Archives and Records Administration regulations. The user and system related information is retrievable by authorized personnel via the server logs based on system specific parameters such as user ID, IP address, and error messages. Audit logs are retained for 12 months online and 18 months offline in accordance with DEA Cybersecurity Standards audit log retention requirement. The DEA File Number (DFN) is a number associated to a particular DEA record series. The DFN below provides mandatory disposition instructions for DARTS 2.0 and DICE 2.0 mission-related and administrative records when no longer needed for business use in accordance with the DEA Records and Information Management System Handbook (DEARIS).

For Disposition: Destroy 10 years after date of report. Earlier destruction is authorized when the files are no longer needed for investigative purposes. Do not transfer files to the Federal records center.

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:

JUSTICE/DEA-008, Investigative Reporting and Filing System, 77 Fed. Reg. 21808 (Apr. 11, 2012)(full text); 82 Fed. Reg. 24151, 156 (May 25, 2017)(amendment).
https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf

DOJ-003, Correspondence Management Systems (CMS) for the Department of Justice, 66 Fed. Reg. 29992 (Jun. 04, 2001)(full text); 66 Fed. Reg. 34743 (Jun. 29, 2001); 67 Fed. Reg. 65598 (Oct. 25, 2002); 82 Fed. Reg. 24147 (May 25, 2017) (amendments).
https://www.govinfo.gov/content/pkg/FR-2001-06-04/pdf/01-13860.pdf

Section 8: Privacy Risks and Mitigation

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

a. Potential Threats Related to Information Collection

Privacy Risk: Individuals may be unaware their PII is being collected and cannot meaningfully consent to the collection of their PII.

Mitigation: This risk is partially mitigated for any PII of the investigators at DEA and HSI by the use of the mandatory banner at login for DEA and HSI T-21 Users. The banner when users are accessing this application states the site is for SENSTIVE processing only. By using this application, the users should be aware they are consenting to monitoring and any unauthorized user is subject to criminal and/civil prosecution and penalties. However, this risk cannot be mitigated with regard to the targets of the investigation whose PII is collected because as the information is acquired pursuant to an active criminal investigation, it is not feasible nor prudent to give notice or obtain consent to collection of their PII.

Privacy Risk: PII may be collected for investigations or activities beyond the scope of DEA's Title 21 authority

Mitigation: This risk is partially mitigated. Input of PII from investigations with no alleged Title 21 violation should not occur since the entire purpose of the DEA T-21 system is to ensure deconfliction between DEA cases, which generally are always predicated on Title 21 authorities, and HSI cases that may begin predicated on non-Title 21 authorities, but where evidence of alleged Title 21 violations is discovered. HSI personnel are provided a reference guide to Title 21, that informs the prospective user of what information is allowed in the system. Only in very limited situations, will DEA investigate non-Title 21 crimes not directly linked to criminal violations of the Controlled Substances Act and those situations would be unlikely to be input into DEA T-21. However, only the allowed documented data can be deconflicted for the DEA T-21 users. Further, the DEA-HSI Interagency Cooperation Agreement is premised on there being some alleged Title 21 violation to deconflict so as to promote efficient coordination of DEA and HSI investigations to ensure officer safety, impact drug trafficking organizations, eliminate duplication of DEA effort, and allow DEA and HSI to work together to reduce the availability of drugs in the United States.

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

Privacy Risk: Authorized DEA personnel may mishandle or fail to safeguard PII.

Mitigation: This risk is partially mitigated. DEA T-21 utilizes numerous security tools to ensure that the components are securely configured and managed in accordance with policy. However, there is still a residual possibility personnel may not handle the PII data in accordance with that policy by DEA personnel. Therefore, DEA users receive annual training on and are expected to follow DEA IT Rules of Behavior that defines PII requirements to the users of DEA's IT systems, including T-21. All users are required to review and provide signature or electronic verification acknowledging understanding of these rules. HSI users are similarly required to receive annual privacy and cybersecurity training, per Federal law and policy.

Privacy Risk: Monitoring, testing and evaluation of privacy and security controls may be insufficient or too infrequent and DEA may not appropriately audit, document, and review compliance of its PII rules on this system.

Mitigation: This risk is mitigated through the completion of the core control review as defined by DOJ and the quarterly review of any outstanding POAMs as defined by DEA. DEA utilizes a standardized build process to ensure all auditing and security tools are implemented in accordance with approved guidelines. Further, DEA's security tool, Crowdstrike, agents manage/monitor the configuration of the systems to validate that auditing is configured in accordance with DOJ/DEA standards. Validating the compliance of PII rules is inherited through the Firebird[5] systems/processes.

Privacy Risk: Data may be retained longer than necessary, which may reduce the relevance and timeliness of the data. This is specifically of concern because DARTS 2.0 and DICE 2.0 system data is consolidated from multiple interconnections receiving data in different file formats, source code languages, and file types. Because of this and without DARTS 2.0 and DICE 2.0 as the authoritative data source, inaccurate data risk can be significant.

[5] Firebird is covered by separate privacy documentation.

Mitigation: This risk is mitigated. Records entered into T-21, while logically separated, reside on the DICE 2.0 system, which controls the retention and disposition of the records in accordance with DEA Records and Information Management System Handbook (DEARIS) with appropriate authority of the National Archives and Records Administration when that is determined. The data entered into the DICE 2.0 applications originate from Law Enforcement investigations. The applications are designed to leverage and aggregate information entered and collected for the purpose of deconfliction between law enforcement entities. Historical data and changes to a subject's data are useful to Law Enforcement investigations. Data received goes through a standardization process to normalize the data to ensure accuracy before uploading into the database for application usage. only what is provided for DEA T-21 can be viewed within the T-21 web application

The DEA File Number (DFN) is a number associated to a particular DEA record series. The DFN discussed in section 6.3 provides mandatory disposition instructions for DARTS 2.0 and DICE 2.0 mission-related and administrative records when no longer needed for business use in accordance with DEARIS.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: The system's administrative controls may be insufficient to prevent unauthorized individuals within DEA and HSI from accessing the system's PII without a need to know.

Mitigation: This risk is partially mitigated. See the discussion of administrative controls in Section 6.2. The Accounts Management system for both agencies are involved in the control for determining user access rights and determining need to know. Upon termination, transfer, or loss of a need to access the system, the controlling agency is responsible for policing access. DEA, resultingly, accepts what HSI represents as their users and their need to know. In addition, the Crowdstrike application and other technical security tools continue to monitor access to data that is available for use by DICE 2.0 and DEA T-21. Risks related to dissemination of information outside T-21 to individuals without a need to know are minimized, as there is no exporting of data through DEA Title 21 web application. Only specific data can be viewed from DICE 2.0 for HSI personnel use through T-21.