Drug Enforcement Administration

Privacy Impact Assessment
for
DEA Enterprise Digital Identification System (DEDIS)

Issued by:
James Robert Bryden
Drug Enforcement Administration

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

Date approved: April 26, 2024

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

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

The Drug Enforcement Administration (DEA) Enterprise Digital Identity System (DEDIS) powered by SailPoint IdentityIQ software (hereafter DEDIS) is a commercial off the shelf (COTS) identity verification and access control management system that condenses and streamlines identity verification management from multiple systems into a single product intended to support the DEA Enterprise. Please note that authentication services are centrally managed through a different system, Okta, and the Firebird infrastructure, but user identity and account information are maintained by DEDIS.

DEDIS is an unclassified internal DEA application that is hosted on and only accessible through DEA's Firebird network.[1] All authorized DEA users (DEA employees, detailees to DEA, DEA task force officers, and DEA contractors) will have a centralized digital identity stored in DEDIS that originates from multiple data sources for consolidation to include user account information and personnel data. DEDIS stores user roles which are based on assigned job functions and approved authorizations. Other DEA personnel-related systems leverage this user roles information for role-based access control.

DEDIS is the technical means by which individuals' gain standard user and privileged user access to many systems that are outside of DEDIS, including various criminal investigation and administrative systems. A user's access, both standard and privileged is based on the roles that the various system owners assign to each individual DEA employee, contractor, task force officer, or other federal employees working at DEA locations. The user role attributes originate from multiple data sources outside of DEDIS, and are consolidated within DEDIS to include user account information and personnel data along with their role-based access permissions. Role-based access to systems, applications, or data are based on their assigned job functions and approved authorizations. DEDIS has its own set of roles to include both standard and privileged; privileged users can administer the DEDIS application.

In addition, DEDIS will function as an account management system that will be used to streamline basic functions to include an automated account request process. DEDIS gives supervisors and managers the ability to manage DEA Information Technology network and application accounts and accesses for their employees, contractors, task force officers, and other federal employees working for DEA, and includes an interactive portal for system administration personnel to track account management requests submitted by supervisors and managers. Authentication for access to DEDIS is centrally managed through Okta and Firebird authentication processes, but user identity along with their information is maintained on DEDIS. DEDIS also provides a dashboard for managers and users to track their identity profile, associated roles, and approved access to system/application resources. DEDIS is responsible for managing user access recertification.

Because DEDIS collects personally identifiable information (PII), DEA has conducted a Privacy Impact Assessment in accordance with Section 208 of the E-Government Act of 2002.

---

[1] DEA will cover the Firebird Network with separate privacy compliance documentation.

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.

DEDIS contains PII (which is described in Section 3.1 below) in support of the Microsoft Active Directory (AD) Authentication process. DEDIS uses Microsoft Windows AD directory services for end-user authentication via any workstation on the network. A "complete trust" domain model has been created to allow this functionality. DEA has implemented Homeland Security Presidential Directive 12 (HSPD-12)[2] for authentication to Firebird workstations and DEDIS/Firebird administrative accounts. The HSPD-12 implementation makes it mandatory for DEA users to use a PIV card to access any DEDIS components. When a user authenticates to AD, the Public Key Infrastructure (PKI) certificate on their PIV card is verified by the DOJ PKI infrastructure.

DEDIS activities encompass all the following sub activities:

- Account management,
- Enterprise architecture, management improvement, and capital planning
- Help desk services and customer services
- Cybersecurity – Automated account management based on predefined security settings,
- System maintenance, contingency planning, continuity of operations, and information technology service recovery.

DEDIS will also obtain information from various sources that include PII. Below is a list of the data source providers to be configured through phase 1:

- DOJ Enterprise Identity Access Management (IAMDOJ) – data feeds for
    - US Access – PIV card serial number and other information
    - Justice Security Tracking and Adjudication Record System (JSTARS) / Security Programs – Clearance status
    - National Financial Center – Human Resources data for government employees
- Firebird – User and privileged user attributes
- CONCORDE – System that consolidates legacy and stove-piped systems into a one-stop data source
- DEA OKTA – Enterprise identity, user credential and access management platform
- Academy Information Systems (ACADIS)
- ServiceNow
- Enterprise Data Warehouse (EDW) – data feeds for
    - DEA Learning System (DEALS) – Training data
    - Table of organization management
    - Web Time and Attendance (WebTA) – DEA Employee and Task Force Officer (TFO) (state and local police) location and supervisor data

The aforementioned systems are all responsible for completing their own privacy reviews.

---

[2] See, https://www.dhs.gov/homeland-security-presidential-directive-12.

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	The Controlled Substances Act, 21 U.S.C. §801, et seq.; the Federal Information Security Modernization Act of 2014, 44 U.S.C. 3551 et seq.; 44 U.S.C. §§3101-3102; 28 U.S.C. §§ 510, 534;
X	Executive Order	Executive Order No. 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017);
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	Privacy and Civil Liberties DOJ Order 0601 Cybersecurity Program DOJ Order 0904; Minimum Security Requirements for Federal Information and Information Systems FIPS PUB 200; NIST Special Publication 800-37 Revision 2; NIST Special Publication 800-53 Revision 5; OMB Circular A-130, Managing Information as a Strategic Resource (2016)

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 and B	User and System Administrative Data
Date of birth or age	X	A and B	Possible collection of date of birth or age information of DEA employees, contractors, TFO Detailees and other Government personnel.
Place of birth			
Gender	X	A and B	Possible collection of Gender information of DEA employees, contractors, TFO Detailees and other Government personnel.

(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
Race, ethnicity, or citizenship	X	A and B	Possible collection race, ethnicity or citizenship information of DEA employees, contractors, TFO Detailees and other Government personnel.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A and B	Will collect SSN#, Name, agency, employer and associated employment info, email address/phone numbers, location, and organizational information of DEA employees, contractors, TFO Detailees and other Government personnel.
Tax Identification Number (TIN)	X	A and B	Possible collection of TIN of DEA employees, contractors, TFO Detailees and other Government personnel.
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A and B	Possible collection of personal mailing address of DEA employees, contractors, TFO Detailees and other Government personnel.
Personal e-mail address	X	A and B	Possible collection of personal e-mail address of DEA employees, contractors, TFO Detailees and other Government personnel.
Personal phone number	X	A and B	Possible collection of personal phone number of DEA employees, contractors, TFO Detailees and other Government personnel.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			

(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
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			
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**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(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
System admin/audit data:	X	A and B	System administrative and auditing data to include user identification and associated passwords, IP addresses and date/time of access and is used for troubleshooting applications, internal DEA access and auditing of DEA employees, contractors, TFO Detailees and other Government personnel.
- **User ID**	X	A and B	Same as above
- **User passwords/codes**	X	A and B	Same as above
- **IP address**	X	A and B	Same as above
- **Date/time of access**	X	A and B	Same as above
- **Queries run**	X	A and B	Same as above
- **Contents of files**	X	A and B	Same as above
Other (please list the type of info and describe as completely as possible):	X	A	Pay plan, job title, employment status, grade, category, series, and step are collected of DEA employees, contractors, and TFO Detailees.

NOTE: System Admin/Audit Data: Auditing information as identified above is collected as part of the process of documenting activity within the software systems used across DEDIS components. Audit logs record the occurrence of an event, the time at which it occurred, the responsible user or service and the impacted entity. All of the devices that encompass DEDIS components emit logs that may be used for auditing purposes. A series of the audit logs is called an audit trail because it shows a sequential record of all the activity that occurred on DEDIS. By reviewing the audit logs, system administrators can track user activity and the security teams (Incident Response Teams) can investigate breaches and ensure compliance with regulatory requirements such as National Institute for Standards and Technology (NIST) 800-53 Rev 5.[3]

DEDIS's audit logs capture the following types of information:

- Event name as identified in the system
- Easy-to-understand description of the event
- Event timestamp
- Actor or service that created, edited, or deleted the event (user ID or API ID)
- Application, device, system, or object that was impacted (IP address, device ID, etc.)
- Source from where the actor or service originated (country, host name, IP address, device ID, etc.)

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

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

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Other Federal entities	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			

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	System admin/Auditing data may be used/shared to troubleshoot issues with applications. Access control data is shared through DEDIS to other applications 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	X		System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
Federal entities	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
State, local, tribal gov't entities	X			System admin/Auditing data information may be required by law enforcement from other organizations for investigations regarding cybercrimes.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X	X		System admin/Auditing data information may be required by law enforcement from other organizations to assist with criminal discovery/investigation.
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.

This system will not release data to the public.

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.

All DEDIS components provide the below generalized notice. All users are presented with the following banner notice prior to logging onto the DEDIS. This banner explains to the user their rights as it pertains to using DEDIS. It should be noted that all users access DEDIS through OKTA which also displays the DOJ approved banner. The banner reads:

> You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:
>
> The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, Communications Security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
>
> At any time, the USG may inspect and seize data stored on this IS. Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. This IS including security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
>
> Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

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 DEDIS. DEDIS is used for managing user access and accounts from various data sources to provide a centralized identity governance solution. DEDIS collects information from various sources that include PII. However, prior to gaining access to this data the users must acknowledge the collection of the PII data and agree to the Privacy Act Statement and Release information, which is detailed in Section 5.1 above.

The audit data collected is for system administrative/troubleshooting purposes. If a user requires auditing information the request should go through the proper channels to include utilizing the helpdesk.

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.

DEDIS users can modify their data using either DEDIS, the DEA service desk or using DEA's Microsoft Identity Manager portal.

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):** Current ATT Date for DEDIS – ATT issued June 5th, 2023 – ATT expiration December 31st, 2023, expected completion date of DEDIS for full ATO is December 31st, 2023. **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 POAM DEDIS has that pertains to privacy controls related to processing this document. Once this document is complete, the POAM 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:** DEDIS was assigned the 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) 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 effect the information system's creation, collection, use, processing,

	storage, maintenance, dissemination, disclosure, or disposal of PII are reviewed and assessed by the Senior Component Official for Privacy prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** DEA Cybersecurity Operations, Response and Engineering Unit (TCVV) is responsible for reviewing and analyzing the DEDIS 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 DEDIS using the Splunk event correlation tool[4] 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**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Required training is distributed and tracked via the DEA Learning Management System – DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and cybersecurity awareness training that are applicable to all DEA component personnel.

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?

Technical privacy and security administrative controls:

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

- 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 information system accounts;
- Establishes conditions for group and role membership;

[4] Splunk is covered by separate privacy documentation here: https://www.justice.gov/d9/2023-01/doj_laas_pia_final_for_publication_1.pdf.

- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by for requests to create information system accounts;
- 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;
- Notifies account managers:
  - When accounts are no longer required;
  - When users are terminated or transferred; and
  - When individual information system usage or need-to-know changes;
- Authorizes access to the information system based on:
  - A valid access authorization;
  - Intended system usage; and
  - Other attributes as required by the organization or associated missions/business functions;
- Reviews accounts for compliance with account management requirements.

Through the utilization of Microsoft 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. The DEDIS components utilize the following technical controls to protect the data:

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

Physical controls:

DEDIS has been deployed in a DEA secured data center. This data center provides physical protection for all hosted systems to include servers, switches, and other devices employed to support the DEA mission. In addition, the data center supplies electrical and HVAC systems for the hosted components. The data center utilizes numerous safeguards to include guards who monitor the facility. Entry includes two sets of doors, the first utilizes 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 DEDIS 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.)

In accordance to NIST 800-53 Rev 5 and the General Records Schedule 3.2: Information Systems Security Records Section Item 060 PKI administrative records will be retained for a minimum of seven years, six months. Longer retention is authorized, if required, for business use.

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/DOJ-002, Department of Justice Information Technology, Information System, and Network Activity and Access Records, 86 Fed. Reg. 37188 (July 14, 2021). https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf

JUSTICE/DOJ-020, DOJ Identity, Credential, and Access Service Records System, 84 Fed. Reg. 60,110 (Nov. 7, 2019). https://www.govinfo.gov/content/pkg/FR-2019-11-07/pdf/2019-24246.pdf

Please note, the following SORNS apply to the systems or subsystems using DEDIS:

- DEA-003, *Automated Records and Consolidated Orders System-Diversion Analysis and Detection System (ARCOS-DADS)*, 69 Fed. Reg. 51104 (Aug, 17, 2004)
- DEA-005, *Controlled Substances Act Registration Records (CSA)*, 52 Fed. Reg. 47182, 208 (Dec. 11, 1987)
- DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (April 11, 2012)
- DEA-010, *Planning and Inspection Division Records*, 52 Fed. Reg. 47182 (Dec. 11, 1987)
- DEA-011, *Operations Files*, 52 Fed. Reg. 47182 (Dec. 11, 1987)
- DEA-012, Registration Status-Investigation Records, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)
- DEA-013, *Security Files*, 52 Fed. Reg. 47182, 215 (Dec. 11, 1987)
- DEA-015, *Training Files*, 52 Fed. Reg. 47182 (Dec. 11, 1987)
- DEA-017, *Grants of Confidentiality Files (GCF)*, 52 Fed. Reg. 47182, 218 (Dec. 11, 1987
- DEA-020, *Essential Chemical Reporting System*, 52 Fed. Reg. 47182, 219 (Dec. 11, 1987)
- DEA-021, *DEA Aviation Unit Reporting System*, 65 Fed. Reg. 24986, 987 (Apr. 28, 2000)
- DOJ-001, *Accounting Systems for the Department of Justice*, 69 Fed. Reg. 31406 (June 3, 2004)
- DOJ-003, *Correspondence Management Systems (CMS) for the Department of Justice*, 66 Fed. Reg. 29992 (June 4, 2001)

- DOJ-006, *Personnel Investigation and Security Clearance Records for the Department of Justice,* 67 Fed. Reg. 59864 (Sept. 24, 2002)
- DOJ-009, *Emergency Contact Systems for the Department of Justice*, 69 Fed. Reg. 1762 (Jan. 12, 2004)
- DOJ-014, *Department of Justice Employee Directory Systems*, 74 Fed. Reg. 57194 (Nov. 4, 2009)
- DOJ-020, *DOJ Identity, Credential, and Access Service Records System*, 84 Fed. Reg. 60110 (Nov. 7, 2019)
- JMD-003, *Department of Justice Payroll System*, 69 Fed. Reg. 107 (Jan. 2, 2004)
- JMD-026, *Security Monitoring and Analytics Service Records*, 86 Fed. Reg. 41089 (July 30, 2021)
- OPM SORN GOVT-1, *General Personnel Records*, 77 Fed. Reg. 79694 (Jun. 19, 2006)
- OPM SORN GOVT-2, *Employee Performance File System Records*, 71 Fed. Reg. 35347 (Jun. 19, 2006)
- OPM SORN GOVT-3, *Records of Adverse Actions, Performance Based Reductions In Grade and Removal Actions, and Terminations of Probationers*, 71 Fed. Reg. 35350 (Jun. 19, 2006)
- OPM/GOVT-5, *Recruiting, Examining, and Placement Records*, 79 Fed. Reg. 16834 (March 26, 2014)
- OPM/GOVT-10, *Employee Medical File System Records*, 75 Fed. Reg. 35099 (June 21, 2010)
- USDA/OP-1, *Personnel and Payroll System for USDA Employees*, 63 Fed. Reg. 4213 (Jan. 28, 1998)
- GSA/GOVT-7, *HSPD-12 USAccess*, 80 Fed. Reg. 64416 (October 23, 2015)

Section 8: Privacy Risks and Mitigation

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

a. Potential Threats Related to The Collection of the Information

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 mitigated by the use of the mandatory banner at login. Individuals are presented with the same banner (which is described in detail above in Section 5.1) indicating that their PII is being collected. Note: collection of the PII within the systems using DEDIS are subject to their own notice requirements, if applicable.

Privacy Risk: Because DEDIS aggregates PII data from many sources collected by multiple organizations and maintained across multiple systems there is a chance of overcollection of data or that some PII collected will not be directly relevant and necessary for the system to accomplish its purpose/mission.

Mitigation: DEDIS developers are actively working with the data owners from the outside organizations to control ingested data. However, this item should be included as part of the Plan of Action and Milestones (POAM) that has been created to ensure that the adopted policy includes data minimization. DEDIS developers are actively working with data owners to develop processes to ensure data minimization is included as part of the onboarding of each connection.

Privacy Risk: Because of the aggregate of data from the various sources as defined in Chart 3.1 above there is a chance that the PII may be used for a purpose or in a manner unrelated to the reason why the information was originally collected.

Mitigation: This risk is partially mitigated. DEDIS developers are actively working with the data owners from the outside organizations to control ingested data. In addition, controls referenced at Section 6.2 have been implemented. The data is controlled through defined access permissions whereby only authorized data is visible based on the role of the user. For example, a standard user can only view their own data and through the use of programmatically defined access controls by the application cannot see other user data.

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

Privacy Risk: Potential susceptibility of system information either at rest or in transmission to compromise from an “Insider Threat” or technological/cyber breach (e.g., Hacking) resulting in a breach.

Mitigation: This risk is mitigated. DEDIS has implemented a Data at Rest and Data in Transit solution which has been validated utilizing security guides. Further there are numerous security tools deployed at critical locations within DEA to ensure any compromise is identified and the DEA Enterprise Incident Response Plan has processes to follow in the case of compromise. See also the measures described above in Sections 6.1 and 6.2

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

Mitigation: This risk is partially mitigated. DEDIS utilizes numerous security tools to ensure that the components are securely configured and managed in accordance to policy. However, there is still a possibility personnel may not handle the PII data in accordance with policy. Additionally, 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. All users are required to review and provide signature or electronic verification acknowledging understanding of these rules.

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. These measures are described above in Sections 6.1 and 6.2. DEA has focused their attention specifically on those that pertain to PII data.

DEA utilizes a standardized build process to ensure all auditing and security tools are implemented in accordance to approved guidelines. Further the Qualys system agent manages/monitors the configuration of the systems to validate that auditing is configured in accordance with standards. Validating the compliance of PII rules is inherited through the Firebird systems/processes.

Privacy Risk: The administrative control environment established for the system may not clearly define the roles and responsibilities of DEA personnel with respect to handling and protecting PII to ensure only authorized access.

Mitigation: This risk is mitigated. As part of completing the annual core control review as defined by DOJ and the quarterly review of any outstanding POAMs as defined by DEA, the roles and responsibilities as defined for both users and managers are validated annually to include not only applicability but to also ensure compliance. Further, the roles and responsibilities documentation are reviewed/reassessed annually. (See Section 6.1, explanation box re: monitoring, or Section 6.2)

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

Mitigation: At the time, this risk will be partly mitigated but will be mitigated in the medium-term. This risk is specifically of concern as DEDIS components are implementing data consolidation from numerous sources through a phased approach. Because of this, without a DEDIS-wide solution, the risk can be significant. Currently, the relevant security and privacy control is assessed as "Other Than Satisfied" for which an associated POAM has been created. This POAM will ensure that a retention solution is adopted.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: The potential exists for DEA personnel to share or disclose PII Information to an inappropriate party, for an improper use, or in a manner inconsistent with the relevant routine uses and DEA/DOJ policy.

Mitigation: This risk is partly mitigated because users of DEDIS are required to review and provide signature or electronic verification acknowledging understanding the rules identified in the DEA IT Rules of Behavior. DEDIS components are an aggregate of data from numerous sources, addressing this risk should be included as part of the POAM that has been created to ensure that the adopted policy includes checks and balances regarding validating use of PII data.

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.

Mitigation: This risk is mitigated. Qualys, along with other security tools, continues to monitor access to data that is available for use by DEDIS. The security tools working alongside user access and training help mitigate this risk. (See Section 6.1 and Section 6.2)

Privacy Risk: PII information may be accessed and altered by for potentially impermissible purposes, thereby affecting the accuracy and reliability of the information.

Mitigation: This risk is mitigated. DEDIS ingests data from other sources. Therefore, if data is altered, the security tools would alarm DEA TCVV. (See Section 6.1, explanation box re: monitoring, or Section 6.2)