Drug Enforcement Administration

Privacy Impact Assessment
for the
Docket Master System

Issued by:
David J. Mudd
Senior Component Official for Privacy
Drug Enforcment Adminstration

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

Date approved: April 27, 2020

(May 2019 DOJ PIA Template)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

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 Docket Master System (DMS) provides case file tracking and docket processing of current and prior Administrative Law Judge (ALJ) decisions and other adjudications by the Agency and federal courts (including court correspondence papers/documents/orders.) DMS also allows for the entry of brief notes related to case logistics. DMS allows authorized employee users to create, edit, and search docket and case file information, enter hearing information and select court room locations. Users can enter judge assignments, upload documents related to adjudications, enter contact information, comments, and motions, orders, and filings. The system also has calendar features that auto display case information and allows users to schedule and track appointments, meetings, and hearing information. The DMS system's data is selected from the internal DEA application menu which the user chooses a case by running a "docket search" query or one of the available reports. There are 17 reports that all contain data and statistics pertaining to the cases. Dockets can be searched by case name, docket number, judge, Order to Show Cause date range, Request for Hearing date range, Case Sent date range, Final Order date range, Case Closed date range, case type, and case status, or any combination of these fields. Information is entered into DMS manually through the "create docket" function, which is a feature of the system that allows data entry of the fields pertaining to a case, which is referred to as a docket. Documents are uploaded and attached to the dockets through the "create docket" and "edit docket" functions. DMS is a system which resides and is accessed via the Drug Enforcement Administration's (DEAs) Firebird general support system and does not share data with any other system or allow emails to be generated. The DMS system does collect and maintain some forms of PII and therefore DEA is required to complete a Privacy Impact Assessment (PIA) for its use of DMS, pursuant to the E-Government Act of 2002 and the Office of Management and Budget's (OMB) implementing guidance (OMB M-03-22).

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.

DMS collects and maintains data related to formal hearings in accordance with the Administrative Procedure Act (5 U.S.C. § 551, *et seq*) in connection with enforcement and regulatory cases brought by the DEA under the Controlled Substances Act (21 U.S.C. § 801, *et seq*) and its attendant regulations (21 C.F.R. § 1300, *et seq*). This information includes: court and correspondence papers, emails and telephone comments, (information is also provided in the Request for Hearing either the respondent's or his/her attorney), court documents and orders (Show Cause and/or Request for Hearing), and the professional names and addresses for each of the involved parties and the office addresses of attorneys representing both the Respondent and the Government.

The Respondent's information may include names (individual, company), vendor and/or company name, address (street, city & zip) telephone and fax numbers as well as the professional (not home) addresses of any attorney(s) involved in the case. This data captured and recorded through an Order to Show Cause court order request is signed by the Diversion Control Assistant Administrator, or by an Immediate Suspension Order signed by the DEA's Acting Administrator.

Representatives for both parties (the Respondent and the Government) file motions throughout the hearing proceedings and the presiding Judge Issues orders as required.

DMS maintains the collection of data and provides access by use of categories through defined tabs, (e.g. correspondence, edit docket, documents) established for the filtering and retrieval of requested data.

For coordinated hearings held within the DEA Hearing Facility in Arlington, VA, pertinent data is submitted via memorandum consisting of names and dates of birth for all non-Government witnesses and attendees. The information is then disseminated to the Office of Security Programs to perform a cursory security review. However, this sensitive information is not added or shared with individuals or agencies and is only scanned into DMS as support documentation. This information is not utilized by the ALJ or the Agency in adjudicating the merits of cases.

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	Administrative Procedure Act §II, 5 U.S.C. § 551-59 (1966); and Controlled Substances Act, I, 21 U.S.C. § 801 *et seq*. (1970).
	Executive Order	
X	Federal Regulation	21 C.F.R. § 1300, *et seq*. (1997).
	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, C, D	Names of administrative law judges, attorney professional names, POCs, business names, such as physicians, nurses, pharmacists, and/or distributors.
Date of birth or age	X	C, D	Scanned document(s) of non-DEA participants (e.g. respondent's attorney, other may include physicians, nurses, pharmacists, and/or distributors etc.)
Place of birth			
Gender			
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			

(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 mailing address	X	C, D	Personal mailing address of non-DEA participants (e.g. respondent's attorney, other may include physicians, nurses, pharmacists, and/or distributors etc.)
Personal e-mail address	X	C, D	Personal e-mail address of non-DEA participants (e.g. respondent's attorney, other may include physicians, nurses, pharmacists, and/or distributors etc.)
Personal phone number	X	C, D	Personal phone number of non-DEA participants (e.g. respondent's attorney, other may include physicians, nurses, pharmacists, and/or distributors etc.)
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			
Certificates			
Legal documents	X	A, C, D	Names of administrative law judges, attorney professional names, POCs, business names, such as physicians, nurses, pharmacists, and/or distributors.
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			

(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
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	X	A, C, D	Names of administrative law judges, attorney professional names, POCs, professional email and business addresses, professional phone numbers, and any other related 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)**			
System admin/audit data:			
- **User ID**			
- **User passwords/codes**			
- **IP address**			

(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
- **Date/time of access**	X	A	Audit logs
- **Queries run**	X	A	Audit logs
- **Content of files accessed/reviewed**	X	A	Audit logs
- **Contents of files**	X	A , B	Audit logs, B category included related scenarios would be in extremely rare cases.
Other (please list the type of info and describe as completely as possible):			

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

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

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

Non-government sources:					
Members of the public		Public media, Internet		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	X	DMS is a standalone system and does not share data. Only authorized users have access to the system.
DOJ Components				
Federal entities				
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.

DMS does not release information to the public for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The DEA Office of Administrative Law Judges is the exclusive forum where all

administrative enforcement cases are adjudicated nationwide. Parties to litigation file documents on notice to each other and requiring Privacy Act notices on this scale would be overly burdensome and confusing. DMS's notice to the public is covered under system of records JUSTICE/DEA-008 *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.govinfo.gov/content/pkg/FR-2012-04-11/pdf/2012-8764.pdf

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.

All privacy information collected is in relation to and for cases. There is no means to allow the individual to consent, but due to the nature of the regulatory requirements, individuals do not have the opportunity to decline having the information provided and entered into the DMS 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 procedures)? If no procedures exist, please explain why.

Individuals may request access to or amendment of their records maintained in DMS through a FOIA and Privacy Act (FOIAPA) request. A FOIAPA request can be made through the DEA FOIA office; however, all information is readily available through the official case file as DMS is the electronic database, which captures all motions and filings related to case. Individuals who are party to a matter before an administrative law judge could potentially also have access to their information via the discovery process.

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):** *ATO received on May 25, 2018 and expires on May 25, 2021.* **If an ATO has not been completed, but is underway, provide status or expected completion date: N/A** **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 POA&M documentation: *N/A, there are no outstanding POAMs for privacy related controls.*
X	**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:** *DMS is a system which resides and is accessed via Firebird, DEA's general support system. Assigned controls and assessments are conducted within DOJs Cyber Security Asset Management, (CSAM) system through the inheritance process.*
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Please specify:** *DMS is a system which resides and is accessed via Firebird, DEA's general support system. Assigned controls and assessments are conducted within CSAM system through the inheritance process.*
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:** *DMS is a system which resides and is accessed via Firebird, DEA's general support system. Assigned controls and assessments are conducted within CSAM through the inheritance process.*
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 contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.*
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** *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?

All ALJ personnel (currently a staff of 10) plus two Attorney Advisors in the Administrator's adjudication support team utilize DMS. Other than DEA Systems Information (SI) employees, authorization for access must be approved by the Chief Administrative Law Judge and the access list is routinely monitored. An audit report is readily available and periodically reviewed to assess which of the authorized adjudication employees have accessed the system. Every new employee at the Office of Administrative Law Judges (LJ) is trained on the use of the system, and the access of every employee who departs LJ is cancelled. DMS is equipped with an audit report "Login Activity" which shows all users who have logged in from current date back to creation of the system.

Application administrators consist of the Chief Administrative Law Judge, hearing office director, and hearing clerk, can authorize access. Users include LJ, some non-ALJ employees specifically tasked with adjudication responsibilities, and some SI personnel charged with addressing system issues. Immediate notification is relayed to the Office of Information Systems for revocation of access when a user or users depart ALJ and/or the Administrator's adjudication support team.

All DEA personnel, and contractors have been cleared to work on the system and comply with the security policies and procedures established by DEA.

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 is retained consistent with applicable law and policy. The disposition standards for the Federal records in these applications are not currently scheduled by NARA, but are pending approval at this time. The proposed retention is 15 years for DEA's DMS based on Civil Litigation and Show Cause. Once the retention schedule is approved, the final retention schedules are available at https://www.archives.gov/about/records-schedule.

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:

DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf.

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

Collecting and maintaining more personal information than necessary to accomplish the Department's official duties is always a potential threat to privacy. The DEA only collects information relevant and necessary for litigation purposes. DMS collects and receives information on individuals, described and outlined in Section 1 and Section 2.1. The information obtained and collected in DMS allows the DEA to keep track of case files and docket processing of current and prior ALJ decisions, as well as other adjudications by the Agency and federal courts. DMS also allows for the entry of brief notes related to case logistics. DMS allows authorized employee users to create, edit, and search docket and case file information, enter hearing information and select court room locations. Users can enter judge assignments, upload documents related to adjudications, enter contact information, comments, and motions, orders, and filings. The system also has calendar features that auto display case information and allows users to schedule and track appointments, meetings, and hearing information.

Further, DMS collects information on court and correspondence papers, emails and telephone comments, (information is also provided in the Request for Hearing either the respondent's or his/her attorney), court documents and orders (Show Cause and/or Request for Hearing), and the professional names and addresses for each of the involved parties and the office addresses of Attorneys representing both the Respondent and the Government. The Respondent's information may include names (individual, company), vendor and/or company name, address (street, city & zip) telephone and fax numbers as well as the professional (not home) addresses of any attorney(s) involved in the case. While a great deal of information is collected about individuals, the vast majority of information is supplied by the courts and/or respondent's attorney. DMS does not provide a privacy notice to individuals because the information collected and maintained is in connection with ongoing cases. The information collected and maintained is necessary to accomplish the DEA's mission.

B. Potential Threats Related to the Use of the Information

Potential threats to privacy as a result of the Department's use of the information in DMS include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information, and unauthorized disclosure of the information.

DEA has established secure worksites to include armed guards, cameras, and restricted Personal Identity Verification card access which also requires a pin for single sign-on to login for the system as well as to gain access to assigned office locations. Obtained access is limited based on a need-to-know requirement and authorization is restricted and monitored tightly by the Administrative Law Judges' office. DMS is only available to authorized users to include the DEA Administrator, the Administrative Law Judges, hearing office director, hearing clerk, law clerks, secretaries, and attorneys in the Administrator's adjudication support team. Authorization must be also be approved by the DEA Chief Judge.

For coordinated hearings held within the DEA Hearing Facility in Arlington, VA, pertinent data is submitted via memorandum consisting of names and dates of birth for all non-Government attendees. The information is then disseminated to the Office of Security Programs to perform a cursory security review. However, this sensitive information is not added or shared with individuals or agencies and is

only scanned into DMS as support documentation. All DEA personnel and contractors have been cleared to work on the system and comply with the security and procedures established by DEA.

C. Potential Threats Related To Dissemination

Using DOJ's CSAM tool, the information type, Personal Identity and Authentication, were identified during the security categorization of the system. This particular information type has a Confidentially, Integrity, and Availably Federal Information Processing Standards (FIPS) 199 rating of Moderate which means the controls regarding privacy are tested to ensure access and protection safeguards are in place to reduce the risk of compromise, including unwarranted access or dissemination of PII. As described in Section 2.1, information is maintained and categorized by the use of categories through defined tabs, which is established for the filtering and retrieval of requested data. Consistent with FISMA and NIST security controls, transmissions of DEA data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), or Secure Sockets Layer (SSL).

DMS is a system that is accessed via Firebird, DEA's general support system which is registered in CSAM. Entry to the system is managed and controlled through single sign-on username/password and based on assigned roles and a need-to-know. An audit report is readily available and periodically reviewed to assess which of the authorized adjudication employees have accessed the system. Every new employee at the Office of Administrative Law Judges (LJ) is trained on the use of the system, and the access of every employee who departs LJ is cancelled. DMS is equipped with an audit report "Login Activity" which shows all users who have logged in from current date back to creation of the system. This will help track individuals who have accessed, input, and/or changed information in the DMS system.

Application administrators authorize access. Users include LJ, some non-ALJ employees specifically tasked with adjudication responsibilities, and some SI personnel charged with addressing system issues. Every new employee at the Office of Administrative Law Judges (LJ) is trained on the use of the system, and the access of every employee who departs LJ is cancelled. Immediate notification is relayed to the Office of Information Systems for revocation of access when a user or users depart ALJ and/or the Administrator's adjudication support team. All DEA personnel and contractors have been cleared to work on the system and comply with the security policies and procedures established by DEA.