Drug Enforcement Administration

Privacy Impact Assessment
for
DEA Disciplinary Management System (DDMS)

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

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

Date approved: July 17, 2025

(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 Office of Professional Responsibility (OPR) for the Drug Enforcement Administration (DEA) conducts investigations of all credible allegations of misconduct levied against any DEA employee, Task Force Officer, or contract employee. Misconduct is generally defined as any violation of Federal, state or local law and/or violation of the DEA's Standards of Conduct.

The DEA Disciplinary Management System (DDMS) provides a powerful suite of case management, human capital management, and risk assessment tools previously unavailable within the Office of Professional Responsibility (OPR). DDMS, which is a cloud-based Salesforce Software as a Service (SaaS) solution, allows for real-time information and data entry, increased information security, and a consolidated repository for all case data.

DDMS is a fully electronic system and a suite of case management, human capital management and risk assessment tools. DDMS permits both the field and headquarters to:

- Combine three existing, legacy databases, transition from fractured data storage practices (i.e. subdirectories and share drives), facilitate the transfer and review of information, create a single system and provide a clear audit trail.

- Enhance the use of data analytics, including data quality and descriptive analytics (dashboard, trends, data visualization)[1]; tools for work unit/individual workload analysis to facilitate timely completion of investigations.

- Provide DEA as an enterprise with the ability to examine misconduct-related trends within the employee population and identify areas of risk for compliance-related policy, training or resource management efforts.

A centralized web-based platform enables all stakeholders to manage employee workload and administrative functions in a seamless and consolidated manner.

[1] Analytic outputs from DDMS do not contain PII.

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.

DDMS is a fully electronic system of records, and a suite of case management, human capital management and risk assessment tools. The system will contain sensitive, but unclassified (SBU) information related to misconduct investigations within DEA OPR. DDMS will collect and maintain personally identifiable information (PII) to include, but is not limited to, name, Social Security number (SSN), position, office assignment and job series of DEA employees and contractors. OPR conducts investigations of all credible allegations of misconduct levied against any DEA employee, Task Force Officer or contractors. Misconduct is generally defined as any violation of Federal, state or local law and/or violation of the DEA's Standards of Conduct.

DDMS is a SaaS system, hosted within the Salesforce GovCloud Infrastructure-as-a-Service and authorized at the Federal Risk and Authorization Management Program (FedRAMP) High level. The main users of the system are DEA OPR and DEA Human Resources. DEA OPR also interacts with the Department of Justice Office of Inspector General (OIG) through DDMS vis-a-vis automated workflow. DDMS forwards all allegations of misconduct to OIG. OIG has the first right of refusal to investigate a case.

OPR referrals are electronically uploaded into DDMS through a intake portal located within DEAs intranet and/or manually by DEA OPR personnel. Data is processed and accessed by DEA employees within the disciplinary system, to include the Office of Professional Responsibility, Board of Professional Conduct, Office of the Deciding Official, Human Resources Employee Relations and Office of Security Programs. Users must have the appropriate roles and permissions, in order to update and modify information within DDMS. Data is disseminated/shared between each stakeholder group through an automated workflow, based on the appropriate case type, role and permission. Updated, modified or deleted case data is documented within the case history identifying the user, date and time.

While DDMS information can be shared, access to the platform is not permitted without the proper roles and permissions provided through traditional access management procedures verifying a user's need to know. The DDMS system administrator provides DEA Chief Counsel access to OPR files for review on a consistent basis. The space used to provide access is called the DDMS Community Space.

Authority		Citation/Reference
X	Statute	21 U.S.C. § 878 and Title 18 of the United States Code entitled "Crimes and Criminal Procedure"

	Authority	Citation/Reference
	Executive Order	
X	Federal Regulation	Title 28, Chapter I, Part 45 of the Code of Federal Regulations (C.F.R.) entitled "Employee Responsibilities"; Title 28, Chapter I, Section 45.735-25, C.F.R. Section 303, Title 5 U.S.C. 5 C.F.R. Part 2635 -- Standards of Ethical Conduct for Employees of the Executive Branch.
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	Names of employees, contractors, other federal government personnel, and/or members of the public (US or non-USPERs) are collected
Date of birth or age	X	A, B, C and D	Date of birth of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.

(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
Place of birth	X	A, B, C and D	Place of birth, of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected
Sex	X	A, B, C and D	Gender is collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
Race, ethnicity or citizenship	X	A, B, C and D	Race information of employees may be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
Religion	X	A, B, C and D	Religion information of employees may be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B and C	Social Security Numbers are collected of employees, contractors, other federal government personnel, and/or members of the public, (US citizens).
Tax Identification Number (TIN)	X	A and B	Government assigned tax identifiers may be collected of employees, contractors and/or other federal government personnel.
Driver's license	X	A and B	Driver's license information of employees, contractors and/or other federal government personnel may be collected
Alien registration number	X	A and B	Such government assigned identifiers may be collected of employees, contractors and/or other federal government personnel.
Passport number	X	A and B	Such government assigned identifiers may be collected of employees, contractors and/or other federal government personnel.
Mother's maiden name	X	A, B, C and D	Mother's maiden name of employees contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Vehicle identifiers	X	A, B, and C	Vehicle identifiers may be collected of employees, contractors, other federal government personnel, and/or members of the public, (US persons).

(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	A, B, C and D	Personal mailing address of employees are collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Personal e-mail address	X	A, B, C and D	Personal e-mail address of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Personal phone number	X	A, B, C and D	Personal phone numbers of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Medical records number	X	A, B, C and D	Medical records number of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Medical notes or other medical or health information	X	A, B, and C	Health related information of employees, contractors, other federal government personnel, and/or members of the public, (US persons) may be collected
Financial account information	X	A, B, C and D	Financial information of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected
Applicant information	X	A, B, C and D	Applicant information may be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
Education records	X	A, B, C and D	Education records of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Military status or other information	X	A, B, C and D	Military-related information of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Employment status, history, or similar information	X	A, B, C and D	Employment related information of employees, contractors, and/or other federal government personnel may be collected.

(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 performance ratings or other performance information, e.g., performance improvement plan	X	A and B	Employment related information of employees, contractors, and/or other federal government personnel. may be collected
Certificates	X	A and B	Certificates of employees, contractors, other federal government personnel, may be collected.
Legal documents	X	A, B, C and D	Legal documents related to employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Device identifiers, e.g., mobile devices	X	A, B, C and D	Electronic device identifiers etc. related to employees, contractors and/or detailees other federal government personnel, and/or members of the public (US or non USPERs) may be collected.may be collected.
Web uniform resource locator(s)	X	A	Web uniform resource locator information of employees, contractors and detailees may be collected.
Foreign activities	X	A, B, C and D	Foreign activities information of employees, contractors, other federal government personnel, and/or members of the public, (US or non USPERs) may be collected
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	Criminal records information of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs). may be collected.
Juvenile criminal records information	X	A, B, C and D	Juvenile criminal records information of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C and D	Civil law enforcement records related to employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs) may be collected.
Whistleblower, e.g., tip, complaint or referral			
Grand jury information	X	A, B, C and D	Information to grand jury information related to employees, contractors, and/or other federal government personnel may be collected

(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
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	Information concerning witnesses to criminal matters related to employees, contractors, and/or detailees may be collected including witness who are members of the public (US or non USPERs).
Procurement/contracting records	X	A	Procurement/contracting records related information of employees, contractors, and/or detailees may be collected.
Proprietary or business information	X	A	System admin/audit related information etc. of employees, contractors, and/or detailees may could be collected.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	Photographs or photographic identifiers could be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
- **Video containing biometric data**	X	A, B, C and D	Video containing biometric data could be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
- **Fingerprints**	X	A, B, C and D	Fingerprints could be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs).
- **Palm prints**	X	A, B, C and D	Palm prints could be collected of employees, contractors, other federal government personnel, and/or members of the public (US or non USPERs)..
- **Iris image**			
- **Dental profile**	X	A	Dental profile could be collected of employees, contractors, and detailees .
- **Voice recording/signatures**	X	A	Voice recording/ signatures. of employees, contractors, and/or detailees may be collected
- **Scars, marks, tattoos**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
- **System admin/audit data:**			
- **User ID**	X	A	User ID of employees, contractors, and/or detailees may be collected.
- **User passwords/codes**	X	A	User passwords/code. of employees, contractors, and/or detailees may be collected.
- **IP address**	X	A	IP address of employees, contractors, and/or detailees may be collected.
- **Date/time of access**	X	A	Date/time of system access by employees, contractors, and/or detailees may be collected.
- **Queries run**	X	A	Queries run by employees, contractors, and/or detailees.
- **Contents of files**			
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	X
Phone	X	Email	X		
Other (specify):					

Non-government sources:					
Members of the public	X	Other DOJ Components	X	Other Federal entities	
Commercial data brokers	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		

Non-government sources:
Other (specify): Private sector entities include law firms acting on behalf of requestors, educational institutions, and news agencies.

Non-government sources:					
Members of the public	X	Public media, Internet	X	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			OPR shares case information with DEA Chief Counsel, Board of Professional Conduct and Deciding Officials Office.
DOJ Components	X			OPR notifies its parent agency (DOJ) of new cases. DOJ Office of Inspector General (OIG) has first-right-of refusal on all DEA OPR cases vis-a-vis an automated workflow.
Federal entities				
State, local, tribal gov't entities	X			OPR may notify a TFO's home agency.
Public	X			OPR findings and/or case files are subject to FOIA requests.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			OPR findings and/or the case file are shared as part of criminal or civil discovery.
Private sector				
Foreign governments				

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.**
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

Information that identifies individuals within DDMS will not be released on data.gov.

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.

Notice has been provided generally through the publication in the Federal Register of the following Systems of Records Notices:

OPR-001, "Office of Professional Responsibility Record Index," 76 Fed. Reg. 66752 (Oct. 27, 2011) (as amended).

JUSTICE/DEA-010, "Planning and Inspection Division Records," 52 Fed. Reg. 47182, 213 (Dec. 11, 1987) (as amended).

DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sep. 24, 2002) (as amended).

DOJ-008, "Department of Justice Grievance Records." 68 Fed. Reg. 61696 (Oct. 29, 2003) (full text), 69 Fed. Reg. 47179 (Aug. 4, 2004), 82 Fed. Reg. 24147 (May 25, 2017) (amendments).

DOJ-018, DOJ Insider Threat Program Records (ITPR), 82 Fed. Reg. 25812 (Jun. 05, 2017) (full text); 82 Fed. Reg. 27872 (Jun.19, 2017) (amendment)

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.

Individuals do not have the opportunity to decline collection or use of their information. OPR information and material may not be distributed outside DEA without the direct authorization of the Deputy Chief Inspector of OPR or designee when there is a specific need for the information to be referred to other agencies for their information and/or action. DEA personnel must comply with the requirements of PIM Section 8302 when directed by an OPR Inspector. Failure on the part of DEA personnel to cooperate with an OPR Inspector during an OPR investigation subjects DEA personnel to disciplinary/adverse action.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

DEA employees or members of the public requesting access to OPR case files would need to file a Freedom of Information Act or Privacy Act request. Both types of requests are processed through the DEA Freedom of Information Act (FOIA) Unit. PII information is redacted when FOIA requests for OPR data are processed for the system. In addition, records under SORN OPR-001 are subject to certain exemptions claimed pursuant to 5 U.S.C. 552a(j)(2), (k)(1), (k)(2), and (k)(5). See 28 C.F.R. § 16.80.

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):** DDMS ATO approved January 5, 2022. **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:** Such information is not released.
	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:

	N/A
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:** DDMS is assigned the security category as defined in FIPS 199 based on the information type, Criminal Investigation and Surveillance, resident on the information system which provides timely and accurate reporting, with the ability to continuously update investigative case files. The information types have designated this system to be a high impact system.
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 reauthorization 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 (SCOP), or a duly authorized official, prior to reauthorization by the Authorization Official. DEA ensures that the appropriate officials are made aware, in a timely manner, of information and the information system when it cannot be appropriately protected or secured, and that such is given a high priority for upgrade, replacement, or retirement.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** The application audit logs are reviewed daily as part of the Cybersecurity Operations, Response and Engineering Unit (TCVV) review process. The Operations & Response team reviews all logs forwarded from DEA systems for suspicious behavior and notifies the system owner/security points of contact of any alerts. Additionally, the program management office performs periodic reviews to ensure user and system behavior comply with all applicable DOJ, DEA, and federal guidelines, policies, and laws. DEACORE is not responsible for dictating the periodic review. The system owner is responsible for complying with all guidelines, policies, and laws; the information system security officer (ISSO) is responsible for validating that users comply with said governance while TCVV enforces actions based upon an infraction (cybersecurity incidents, policy violations). TCVV performs validation for compliance to governance during risk assessments which

	are scheduled (ATO renewal or continuous monitoring audit) or remediation efforts against the system during a cybersecurity investigation.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Yes, all contracts have the necessary, proper, and accurate privacy and security-related clauses (i.e., DOJ Clause 02, *Contractor Privacy Requirements*; and DOJ Clause 05, *Security of Information and Information System*) 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:** Privacy Act training is conducted annually and throughout the year in order to provide an overview of agency employees' obligations to protect PII. The component has a requirement for all employees, including contract employees, to complete the mandated Cyber Security Awareness Training annually which has a privacy act component. Additionally, DEA has required role-based, annual refresher privacy trainings for all staff. Required training is distributed and tracked via the DOJ Learning Management System DEALS. This training includes general mandatory annual trainings for information systems like rules of behavior and Cyber Security awareness training that are applicable to all DEA component personnel. DDMS Users are trained on system specific uses of the system through a train-the-trainer program within each stakeholder segment.

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?

DDMS is securely housed and monitored on the Salesforce government cloud with a FedRAMP HIGH classification. The physical controls required to access DDMS consist of a PIV card, Firebird laptop, and government PIV provisioning to DDMS. Technical control for access requires a Salesforce license, federation ID, and profile within the cloud. Administrative controls require an employee to have a security clearance, be assigned to OPR and obtain the necessary user and privilege management.

Privacy and Security Administrative Controls: As part of privacy and administrative controls, the Awareness and Training (AT) control has been implemented for the system. All DEA system users are mandated to take annual training on DOJ cybersecurity Awareness Training (CSAT). The implementation of this control helps employees to be

informed and be vigilant to any potential cybersecurity concerns that may arise. The training also helps employees follow the required procedures and report a cyber incident immediately when it happens. Once DDMS becomes operational, this compliance requirement will be maintained. DEA is requiring the vendor to adhere to strict access controls to ensure only authorized users have access to the data. DDMS is required to maintain effective continuous monitoring activities. For an individual to access DDMS, the individual must be an employee of DEA, OPR, must have a security clearance and Need-to-Know the information to perform their job duties.

Technical control: DDMS users will be granted access based on their permission. For instance, privileged users will have a different access right as compared to general users. This will help to prevent privilege creep as well as privilege escalation which could undermine DDMS' cybersecurity posture. OPR personnel undertakes monitoring, testing, and evaluation to safeguard the information and prevent its misuse. DDMS System Admin utilize monthly user login reports to assess user permission and roles within each stakeholder's compartmentalized space.

Physical Control: Physical and Environmental controls are enforced across all DOJ's buildings as part of its common control requirements. This is enforced with defense in depth. All DEA buildings are fenced with security guards at the entrance of the offices. In addition, employees are required to authenticate with their Personal Identity Verification (PIV) cards before being granted access to enter the building. Access to the system will be based on the need to know which requires authentication via the PIV card as well. All the virtual servers for the system will be secured and backed up to ensure effective cyber hygiene.

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.)

Records are retained and disposed of in accordance with the National Archives and Records Administration's (NARA) General Records Schedule. DDMS follows the NARA approved DEA-specific retention for electronic surveillance policy for keeping records per the DEA Records Information System Handbook, File Number 201-03 (DAA-0170-2017-0007-0003)

Integrity Case Files: Reports related to investigations by the Office of Professional Responsibility, involving criminal or civil violations of laws, departmental codes, or DEA regulations, and integrity and security matters. May include but is not limited to records related to: personnel integrity, polygraph examinations, accidents and incidents, adverse actions, and positive drug test results.

Disposition: Temporary. Cut-off at close of case. Destroy 20 years after close of investigation or 1 year after close of investigation, if investigation remained open beyond 20 years.

However, disposition is not authorized currently due to a litigation hold (Segar v. Bell, 1977 US Dist.) Cases pertaining to 1811 personnel will be retained until the preservation requirement is vacated by court order. Once vacated, DEA will comply with the disposition instructions above. Additionally, hard copies of investigative case files are retained for a period of no more than three years within OPR HQ and subsequently forwarded to the National 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:

OPR-001, "Office of Professional Responsibility Record Index," 76 Fed. Reg. 66752 (Oct. 27, 2011) (as amended).

DEA-010, "Planning and Inspection Division Records," 52 Fed. Reg. 47182, 213 (Dec. 11, 1987) (as amended).

DOJ-006, Personnel Investigation and Security Clearance Records for the Department of Justice, 67 Fed. Reg. 59864 (Sep. 24, 2002) (as amended).

DOJ-008, "Department of Justice Grievance Records." 68 Fed. Reg. 61696 (Oct. 29, 2003), 69 Fed. Reg. 47179 (Aug. 4, 2004) (full text), 82 Fed. Reg. 24147 (May, 25, 2017) (amendments).

DOJ-018, DOJ Insider Threat Program Records (ITPR), 82 Fed. Reg. 25812 (Jun. 05, 2017) (full text); 82 Fed. Reg. 27872 (Jun.19, 2017) (amendment)

Section 8: Privacy Risks and Mitigation

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

a. Potential Threats Related to The Collection of the Information.

Privacy Risk: Individuals may be unaware their PII is being collected and cannot meaningfully consent to the collection of their PII nor participate in collection, use, or dissemination of their PII in this system.

Mitigation. This risk is partly mitigated. DEA employees are generally made aware that there is no expectation of privacy in their use of government provided computers and electronic devices. No other individualized notice is provided, unless individuals are notified through other systems/applications prior to information being entered into DDMS. Because this system is used for law enforcement referral purposes and contains sensitive information related to criminal and administrative investigations, it is not feasible or advisable to provide notice to individuals at the time their information is accessed by the system. No notification beforehand can be accommodated due to the risk of compromising ongoing investigations. DEA keeps track of the details of DDMS entries for subsequent notification in discovery in both civil and criminal cases.

When law enforcement agents and officers interact with DEA personnel in connection with an investigation, however, the subjects are generally aware that their information will be recorded and stored. Furthermore, information collected from outside DEA facilities are obtained through other lawful means, such as by subpoenas and search warrants.

Privacy Risk: DEA may upload inaccurate or non-relevant information into DDMS, affecting both case management and DDMS analytic outputs.

Mitigation: This risk is fully mitigated. DDMS users only upload data that is strictly necessary and corresponding to the investigation. Data validation protocols are in place at OPR and are continually enhanced by incorporating manual checks within the DDMS workflow to ensure accuracy at the point of upload and throughout data processing. OPR deploys regular quality control and monitoring mechanisms within DDMS to automatically identify data inaccuracies. Moreover, DDMS analytic outputs (e.g. dashboards, visualizations) do not contain PII and would not have a detrimental effect on individuals.

Privacy Risk: DEA may collect the PII of an unrelated individual (who is not under suspicion or the subject of investigation) and then becomes part of an incident or investigation about someone else.

Mitigation: This risk is partially mitigated. The PII contained within DDMS cases/files mainly focus on a particular DEA staff member for whom there was sufficient predicate to open a matter. Such files, of course, may contain some PII of supervisors or subordinates or other personnel who may be witnesses to actions under investigation. If information is found not to be relevant, it will be archived in the case file information by the investigating inspector.

Privacy Risk: DDMS may maintain more personal information than necessary to accomplish the DEA's official duties and to accomplish its mission.

Mitigation: This risk is partially mitigated. DEA collects only the amount of information necessary to meet its administrative and criminal investitive purposes. The following measures help ensure that information collected is both relevant and necessary for the investigation: (1) extensive training on the proper collection of relevant information given to criminal investigators; (2) investigative procedures and policies detailing the proper collection of information; and (3) supervisory involvement in all aspects of the investigation, including collection of information.

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

Privacy Risk: DEA may use PII for a purpose or in a manner unrelated to the reason why the information was collected.

Mitigation: This risk is fully mitigated. Personnel will not have access without a need to know. Individuals who access a given file do so with a "need to know" as directed by a supervisor or that develops in the course of performing their duties. DDMS users are made up of administrators and end users (Special Agents, Intelligence Research Analysts and Program Analysts). Administrators are mainly government employees and may be contractors as well that are responsible for system maintenance, backup, restoration, system architecture, development, training and end user support. DDMS utilizes strict access controls at both the database and application layers using the principle of least privilege to provide access on an as-needed basis. Roles are designated to ensure that end users view only the appropriate subsets of data. Only stakeholders (i.e., Office of Professional Responsibility (OPR), Board of Professional Conduct (HRB), Office of the Deciding Official (HRO), Human Resources Employee Relations (HRER) and the Office of Security Programs (IS)) have access to the data of a subject of investigation. Full access control is limited to system administrators who have acknowledged the DEA IT Rules of Behavior prior to gaining that access. Additionally, access to the use of DDMS is not granted to individuals unless they have been vetted and justified to have access.

Further, the information in DDMS is collected for purposes of internal investigations of DEA personnel and may result in criminal referrals, therefore, any use of information from criminal files that is compatible with law enforcement purposes is a legitimate use. DEA policy restricts sharing of such information to the Office of Professional Responsibility and partnering or requesting law enforcement agencies under a published routine use, Privacy Act exception or properly noticed exemption to ensure that the use of this information is consistent with the original professional responsibility and law enforcement purposes for which DEA originally collected the data. Any dissemination to

outside agencies would generate a DEA-381 Disclosure Account Record, in which sharing is logged and justified.

Privacy Risk: Outsiders may access DDMS due to insufficiently implemented Physical, Technical, and Administrative security and privacy controls.

Mitigation: This risk is fully mitigated through proper implementation of the security and privacy controls referenced above in Section 6.2. Further, DDMS is protected from insider threats and malicious, external engineering attacks by DEA's threat monitoring technology. In addition, DEA uses the following governance and audit metrics:

i. While DDMS links can be shared, access cannot. Individuals receiving links will not be able to access the information due to not having initial access. System administrators have the ability to file share only with Chief Counsel and DEA subjects when required.

ii. Audit reports can provide details on login/login attempts by DDMS users to sites, pages and information.. Login roles and permissions are monitored on a weekly basis.

iii. Governance policies mandate that DDMS administrators monitor the platform for unusual activities. DDMS administrators are trained in monitoring and maintenance.

c. Potential Threats Related to Dissemination of the Information

Privacy Risk: Sensitive information within DDMS may be improperly shared outside DEA or access granted to DEA employees who may not have a clearance or need to know for that information.

Mitigation: This risk is fully mitigated. The information is only used by approved stakeholders within the disciplinary system, Office of Professional Responsibility (OPR), Board of Professional Conduct (HRB), Office of the Deciding Official (HRO),Human Resources Employee Relations (HRER) and the Office of Security Programs (IS) to manage caseload and administrative functions in a seamless and consolidated manner. The sharing and use of the data are governed by DEA privacy guidance. An authorized user's access is limited, controlled and tracked by the system. A user is granted access to DDMS data based on the defined role for which they have been approved. Access to pertinent information is strictly limited. This is done to limit the level of privacy intrusions on the target of an investigation.

The system architecture prevents external dissemination of information, ensuring the data remains securely contained. DDMS does not integrate with any external

Application Programming Interfaces (APIs). By maintaining a close ecosystem, DDMS mitigates the risk of data exposure outside of DEA, unauthorized access, and other potential vulnerabilities. In addition, by not relying on external APIs, DDMS eliminates the risks associated with dependency on external services, ensuring security protocols and data access controls remain fully under DEA management.

The case data is stored in government facilities with access control measures in place. Within these facilities, the physical components of the system necessary for end users to access the viewing and analysis tools are stored in controlled areas and restricted to only authorized stakeholders. The lawfully collected data is logically protected from unauthorized viewing and copying by computer login restrictions which permit only authorized users to have access to the data as well as specific permission-based access restrictions at both the application interfaces and the file level. The system is accessed by users with unique and attributable accounts from within government facilities. The system is remotely accessed by a limited number of system administrators via a Virtual Private Network (VPN) connection and a two-factor authentication process. These disseminations are done consistently with DOJ policy and applicable laws and regulations. Further the disseminations are shared only with those authorized to receive them for legal and authorized purposes. Consistent with FISMA and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., (VPN), Secure File Transfer Protocol (FTP), Secure Sockets Layer (SSL), or another encryption. Information is shared on a need-to-know basis only, and via email, mail, facsimile, or phone in accordance with Department policies.

When DEA shares case data within the Department, other components are required to conform to Department policies to prevent or mitigate threats to privacy through disclosure, such as maintaining the integrity of application. Privacy Act protected information, that is, records responsive to requests that contain any PII, is sent to requesters via encrypted e-mail.

Further, all users, both administrators and end users, of the system must obtain certification on a yearly basis by completing DEA Cybersecurity Awareness Training and agree to the IT Rules of Behavior for use of DEA information systems.