Civil Rights Division

Privacy Impact Assessment
for the
CRT-Case Management Database (CMD)

Issued by:
Kilian Kagle, 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: March 20, 2026

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Department of Justice (DOJ or Department) Civil Rights Division (CRT) Case Management Database (CMD) represents a comprehensive legal case management tool that will capture the full panoply of data the litigating Sections of the Civil Rights Division require to successfully pursue their enforcement work. This data may include personally identifiable information (PII) such as names, addresses and contact information of the parties, victims, witnesses, partner agencies, staff, Social Security numbers, Employee Identification Numbers, Alien/Residency Numbers, Voter Identification Numbers, Taxpayer Identification Numbers, Student Identification Numbers, Tax Return Information, protected health information, disability scheduling, and all other data deemed essential by the Division's CMD users. CRT has prepared this Privacy Impact Assessment in accordance with Section 208 of the E-Government Act of 2002.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The CRT has integrated ReconELM, a legal case management solution hosted on the Salesforce FedRAMP High-compliant Software as a Service (SaaS) cloud infrastructure, to build CRT's new Case Management Database (CMD). CMD is a case management system for CRT's management and staff that provides a comprehensive and user-friendly platform for streamlining matter creation and organization, optimizing time keeping, enhancing collaboration, providing actionable information and reporting, and maximizing efficiency. CMD provides legal case management through modules that provide data-driven decision-making, resource allocation, and comprehensive reporting mechanisms. CMD will provide CRT with the ability to have timely data updates, intricate tracking mechanisms, precise time entry, adaptable reporting, and advanced data export capabilities for in-depth evaluations. CMD also enables data sharing through diverse channels, provides extensive documentation for user guidance, and ensures adaptability to evolving data requirements, while aligning with DOJ's enterprise cybersecurity architectures and protocols.

CMD is a web-based application that is accessible across various desktop browsers and offers basic functionality on mobile devices. The system provides robust security features, including individualized secure logins, Single Sign-On integration with DOJ CRT's Identity Provider, and user access determined by assigned security groups.

CMD will allow CRT staff to enter, categorize, and edit time spent on work activities, with specific functionalities tailored to attorneys, such as associating a unique record identifier (DJ Number) to a time entry. The system will also support the creation of DJ Numbers for cases or matters, ensuring data integrity. CMD also will enable users to associate multiple due dates with activities or link multiple investigations to a single target. The application will also be

equipped with features to upload documents, send email notifications for critical events, and maintain an automated activity log for core entities.

CMD will offer advanced reporting capabilities, allowing users to generate detailed reports based on specific data fields. Users will have the flexibility to save, share, and download these reports. The application will also support custom, read-only reporting queries and allow configuration of reporting templates on a per-user basis.

CMD will permit designated CRT personnel to set automated business and workflow rules, assign users to specific user groups, and control access to case records based on group membership or individual criteria. The system will be integrated with DOJ's Microsoft Active Directory, providing real-time monitoring insights, and the ability for CRT IT support staff to impersonate a user for troubleshooting purposes.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority	Citation/Reference
Statute	● Official Misconduct, 18 U.S.C. §§ 241, 242 ● The Matthew Shepard and James Byrd, Jr., Hate Crimes Prevention Act of 2009 ● Federally Protected Activities, 18 U.S.C. § 245 ● Criminal Interference with Right to Fair Housing, 18 U.S.C. § 3631 ● Damage to Religious Property, 18 U.S.C. § 247 ● Trafficking Victims Protection Act (TVPA) ● Freedom of Access to Clinics Entrances Act (FACE) ● Criminal Protection for Voting Rights, 18 U.S.C. § 594 ● Americans with Disabilities Act, Title I ● Americans with Disabilities Act, Title II ● Americans with Disabilities Act, Title III ● Rehabilitation Act of 1973 ● Civil Rights Act of 1964, Title VII ● Uniformed Services Employment and Reemployment Rights Act (USERRA) ● Civil Rights Act of 1964, Title IV ● Equal Education Opportunities Act of 1974 (EEOA) ● Individuals with Disabilities in Education Act (IDEA) ● Civil Rights Act of 1964, Title VI ● Education Amendments of 1972, Title IX ● Civil Rights Act of 1964, Title II ● Fair Housing Act (FHA) ● Equal Credit Opportunity Act (ECOA) ● Religious Land Use and Institutionalized Persons Act (RLUIPA) ● Servicemembers Civil Relief Act (SCRA)

	● Immigration and Nationality Act § 274B ● Civil Rights of Institutionalized Persons Act (CRIPA) ● Violent Crime Control and Law Enforcement Act § 14141 ● Omnibus Crime and Safe Streets Act ● Voting Rights Act ● Voting Accessibility for the Elderly and Handicapped Act ● Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ● National Voter Registration Act (NVRA) ● Genetic Information Nondiscrimination Act (GINA), Title II ● Help America Vote Act (HAVA) ● Civil Rights Acts of 1870, 1957, 1960, & 1964
Executive Order	
Federal regulation	
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, D	Contact records are created in the system and are usually related to legal matter (Case) records.
Date of birth or age	X	A, B, C, D	Information related to Case/Matter
Place of birth	X	A, B, C, D	Information related to Case/Matter
Sex	X	A, B, C, D	Information related to Case/Matter
Race, ethnicity, or citizenship	X	A, B, C, D	Information related to Case/Matter
Religion	X	A, B, C, D	Information related to Case/Matter
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	Information related to Case/Matter
Tax Identification Number (TIN)	X	A, B, C, D	Information related to Case/Matter
Driver's license	X	A, B, C, D	Information related to Case/Matter
Alien registration number	X	A, B, C, D	Information related to Case/Matter
Passport number	X	A, B, C, D	Information related to Case/Matter
Mother's maiden name	X	A, B, C, D	Any PII may be collected as part of a case file.
Vehicle identifiers	X	A, B, C, D	Information related to Case/Matter
Personal mailing address	X	A, B, C, D	Information related to Case/Matter
Personal e-mail address	X	A, B, C, D	Information related to Case/Matter
Personal phone number	X	A, B, C, D	Information related to Case Matter
Medical records number	X	A, B, C, D	Information related to Case/Matter
Medical notes or other medical or health information	X	A, B, C, D	Information related to Case/Matter
Financial account information	X	A, B, C, D	Information related to Case/Matter
Applicant information	X	A, B, C, D	Any PII may be collected as part of a case file.
Education records	X	A, B, C, D	Information related to Case/Matter
Military status or other information	X	A, B, C, D	Information related to Case/Matter
Employment status, history, or similar information	X	A, B, C, D	Information related to Case/Matter
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C, D	Information related to Case/Matter
Certificates	X	A	This data is created and stored by system automatically.
Legal documents	X	A, B, C, D	Information related to Case/Matter
Device identifiers, e.g., mobile devices	X	A, B, C, D	Information related to Case/Matter
Web uniform resource locator(s)	X	A	This data is created and stored by the system automatically.

(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	X	A, B, C, D	Information related to Case/Matter
Juvenile criminal records information	X	A, B, C, D	Information related to Case/Matter
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	Information related to Case/Matter
Whistleblower, e.g., tip, complaint, or referral	X	A, B, C, D	Information related to Case/Matter
Grand jury information	X	A, B, C, D	Information related to Case/Matter
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	Information related to Case/Matter
Procurement/contracting records	X	A, B, C, D	Information related to Case/Matter
Proprietary or business information	X	A, B, C, D	Information related to Case/Matter
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	Information related to Case/Matter
Biometric data:	X	A, B, C, D	Information related to Case/Matter
- **Photographs or photographic identifiers**	X	A, B, C, D	Information related to Case/Matter
- **Video containing biometric data**	X	A, B, C, D	Information related to Case/Matter
- **Fingerprints**	X	A, B, C, D	Information related to Case/Matter
- **Palm prints**	X	A, B, C, D	Information related to Case/Matter
- **Iris image**	X	A, B, C, D	Information related to Case/Matter
- **Dental profile**	X	A, B, C, D	Information related to Case/Matter
- **Voice recording/signatures**	X	A, B, C, D	Information related to Case/Matter
- **Scars, marks, tattoos**	X	A, B, C, D	Information related to Case/Matter
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C, D	Information related to Case/Matter
- **DNA profiles**	X	A, B, C, D	Information related to Case/Matter
- **Other (specify)**	X	A, B, C, D	Information related to Case/Matter
System admin/audit data:	X	A	This data is created and stored by the system automatically.
- **User ID**	X	A	This data is created and stored by the system automatically.
- **User passwords/codes**	X	A	This data is created and stored by the system automatically.

(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
- **IP address**	X	A	This data is created and stored by the system automatically.
- **Date/time of access**	X	A	This data is created and stored by the system automatically.
- **Queries run**	X	A	This data is created and stored by the system automatically.
- **Contents of files**			
Other (please list the type of info and describe as completely as possible): Other categories of PII	X	A, B, C, D	Any PII may be collected as part of a case file.

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

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

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

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	CRT users have direct access to CMD to successfully pursue their enforcement work.
DOJ Components				
Federal entities	X			CRT may share case information and collaborate with other federal entities on a case-by-case basis.
State, local, tribal gov't entities	X			CRT may share case information and collaborate with state, local, or tribal entities on a case-by-case basis.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

No information is released 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.

Individuals' data are gathered through court order, warrant, subpoena, discovery request, and other such methods. In most cases, information about individuals may be contained in documents collected from various parties during litigation. To the extent individualized notice is required by law, court rules, or DOJ policy, the Department will provide varying degrees of direct notice to individuals whose privacy interests are implicated by these orders/requests. Opposing counsel or the court may also provide individualized notice, depending on the circumstances. The Department, however, is not required to provide individualized notice to everyone whose PII may be implicated. That said, individuals are provided generalized notice of the Department's maintenance of these records through the Department's SORNs. The applicable SORNs include JUSTICE/CRT-003.

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.

No such opportunities will be made available to individuals at this system level. As this system is a case management platform and in itself does not collect information but merely tabulates data already resident in other CRT information systems. As such, the information system is a transfer system that does not originate PII. Therefore, the information system will not provide notice or consent to specific uses of information collected beyond those already enumerated in CRT-003.

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.

A request for access to a record retrievable in this system shall be made in writing, with the envelope and letter clearly marked "Privacy Access Request." Include in the request the full name of the individual involved, his or her current address, date and place of birth, and notarized signature or dated signature submitted under penalty of perjury (28 CFR 16.41(d)), and any other information which is known and may be of assistance in locating the record. The requester should provide a return address for transmitting the information. Access requests should be directed to FOIA/PA Branch, Civil Rights Division, 4CON, Room 6.153, 950 Pennsylvania Ave, N.W., Washington, DC 20530 or CRT.FOIArequests@usdoj.gov.

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):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** 7/3/2025 **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:**
	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:** The security categorization for the CMD system is designated as high, as defined in FIPS 199, which evaluates the potential impact on organizational operations should the system's security be compromised. The "high" designation is appropriate given the system's role as a centralized repository for the CRT enterprise-wide security artifacts and real-time monitoring data. Under the FIPS 199 framework, a high impact rating is applied when the loss of confidentiality, integrity, or availability could result in catastrophic adverse effects, such as the total loss of the CRT's mission-essential function or significant damage to national security interests.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** CMD integrates with DOJ's Splunk Enterprise[1], which provides an audit trail that supports real-time threat detection. Every event—ranging from system-level configuration changes to the generation of security artifacts—is immediately ingested, allowing CRT to maintain total visibility over the environment without the delays associated with batch processing or manual uploads. At the data level, CMD tracks granular activities such as file integrity changes, database queries, and administrative access through advanced auditing hooks. These specific data-level events are mapped directly to the CRT Splunk Dashboard, which serves as a centralized, operational command center functioning on a 24x7 basis**.**
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:** To ensure strict adherence to security and privacy standards, auditing procedures are conducted through a hybrid approach of automated analysis and manual oversight. While

[1] Splunk is covered by separate privacy documentation available here: https://www.justice.gov/opcl/media/1363231/dl?inline.

	Splunk provides 24/7 automated monitoring and alerting for immediate anomalies, formal manual reviews of the logs and dashboard metrics are performed by the CRT security team at least once per shift. This rigorous review cycle is supplemented by comprehensive weekly and monthly audit reports generated directly from Splunk to validate compliance with the System Security and Privacy Plan (SSPP). By maintaining this continuous loop of data ingestion, automated flagging, and human analysis, the CMD system ensures that all forensic artifacts remain protected and that every system interaction is fully accountable.
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:** X General information security training X Training specific to the system for authorized users within the Department. X Training specific to the system for authorized users outside of the component.

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?

CMD implements Role-Based Access Control (RBAC), ensuring that access to sensitive data is restricted to authorized personnel based on the principle of least privilege. To detect potential unauthorized access or "privilege creep," the DOJ CRT performs regular auditing of these roles as prescribed by NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems[2], Control AU-6 (Audit Review, Analysis, and Reporting). By generating automated Splunk reports that cross-reference user activity with authorized permissions, the organization can identify and remediate anomalous access patterns, ensuring that only users with a verified "need-to-know" can access CMD data. System users may include:

- Front-Line Staff: Attorneys, paralegals and support staff (PASS) who enter their time spent on matters/cases and other work functions.
- Case Management Staff: Support staff who process matter/case intake and track matter/case workflows.
- IT Support: Includes application developers, system security engineers, system, and database administrators for troubleshooting.
- CRT Counsel: Attorneys in CRT or other DOJ attorneys who have ad hoc reporting needs for audit and oversight matters.
- Division Management: Managers, data analysts, and front office leadership and staff

[2] NIST 800-53 is available here: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

who consistently report on various metrics to DOJ and external entities, including caseloads, docket reviews, and timesheet reports.

- Section Management: Section chiefs and deputies who also have consistent reporting needs, along with some time entry needs.

To secure PII in transmission, the system utilizes Control SC-8 (Transmission Confidentiality and Integrity), which mandates the use of FIPS 140-2/[3] validated cryptographic modules and transport layer security (TLS) 1.2/1.3 encryption protocols[4]. This ensures that any data moving between the CMD system and Splunk is shielded from interception or "man-in-the-middle" attacks. Furthermore, the environment utilizes Control SI-4 (Information System Monitoring) to maintain robust intrusion detection capabilities. These sensors monitor network traffic and system behavior in real-time, specifically looking for indicators of data exfiltration or unauthorized access to CMD. When an anomaly is detected, the system triggers an immediate alert on the CRT dashboard, allowing for a rapid response under Control IR-4 (Incident Handling).

Physical security serves as the final layer of defense, ensuring that the hardware processing CMD data is inaccessible to unauthorized actors. In accordance with Control PE-3 (Physical Access Control) and Control PE-6 (Monitoring Physical Access), the servers and Splunk indexers are housed in data centers protected by biometric authentication and 24/7 video surveillance. Physical isolation is complemented by Control MP-6 (Media Sanitization), which requires that any storage media containing PII be cryptographically erased or physically destroyed before disposal. By integrating these specific NIST controls into a unified defense-in-depth strategy, the CMD system minimizes the risk of unauthorized disclosure and ensures that the privacy of individuals is maintained throughout the continuous monitoring process.

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 maintained in the system while current and required for official government use. When no longer needed on an active basis, the records are stored in accordance with Departmental security regulations for systems of records. The disposition schedule currently assigned is PERMANENT Cutoff at the close of case, transfer to NARA 25 years after cutoff pursuant to DAA-0060-2024-0014 (Litigation Case Status Systems).

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

---

[3] FIPS 140-2 is available here: https://csrc.nist.gov/pubs/fips/140-2/upd2/final.
[4] TLS provides privacy and data integrity between two communicating applications. For more information see: https://csrc.nist.gov/glossary/term/transport_layer_security.

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/CRT-001, Central Civil Rights Division Index File and Associated Records, 68 FR 47610, 611 (8-11-2003),

JUSTICE/CRT-003, Civil Rights Interactive Case Management System, 68 FR 47610, 613 (8-11-2003),

JUSTICE/CRT-004, Registry of Names of Interested Persons Desiring Notification of Submissions Under Section 5 of the Voting Rights Act 68 FR 47610, 614 (8-11-2003),

JUSTICE/CRT-007, Files on Employment Civil Rights Matters Referred by the Equal Employment Opportunity Commission, 68 FR 47610, 615 (8-11-2003).

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.***

Privacy Risk: Unauthorized access or misuse of information

Mitigation: DOJ employs a robust physical security system to protect its servers and access terminals, including secure worksites, armed guards, cameras, and access restricted office suites. CMD also implements access monitoring, privacy and records controls standardized by the NIST Special Publication 800-53.

Employee access to this system is limited based on a need-to-know and further delimited by restrictions which limit users to the minimum access needed. Once those criteria are met and management approval is received, access is granted. This system utilizes a user's Personal Identity Verification (PIV) card and pin number for authentication. It also has been evaluated and authorized to operate according to the risk management framework required by the Federal Information Security Modernization Act of 2014 (FISMA). An audit log is maintained of all user logins and actions. Notification of the monitoring is presented clearly when logging into the system.

Additionally, DOJ employees and contractors must complete annual training regarding handling of PII as part of the Department's Cyber Security and Awareness Training (CSAT), as well as read and agree to comply with DOJ Information Technology Rules of Behavior. This occurs during their orientation upon entering into service with DOJ, and annually thereafter. Additionally, the Division upon request provides one-on-one training for employees granted access to CMD. The Division maintains an Account Management Guide and Configuration Management Guide for CMD. The CMD system assessment is documented in the DOJ Joint Cybersecurity Authorization Management (JCAM) assessment tool and maintained as part of the DOJ ongoing authorization and assessment plan. All security controls are documented in the System Security and Privacy Plan recorded in the IT system. There is no outside access to this system; administrator access is restricted to the few DOJ employees and contractors who administer the program.

Privacy Risk: Name association with the database

Mitigation: As in most cases where a record associates a person with a criminal or civil investigation, the mere presence of a name in the system can generate the assumption of involvement with unsavory activity or other damage to their reputation. For this reason, there is no automated dissemination of information from this system outside of the Division. Any dissemination must be done pursuant to proper authority and management review. Information obtained from this system is considered law enforcement sensitive. Additionally, de-identification of management reporting is practiced in all instances possible.