Criminal Division

Privacy Impact Assessment
for the
Docket Case Management System

Issued by:
Raymond Hulser
Criminal Division, Senior Component Official for Privacy

Approved by: Peter A. Winn, Acting Chief Privacy and Civil Liberties Officer, Department of Justice

Date approved: [August 28, 2018]

(May 2015 DOJ PIA Form)

EXECUTIVE SUMMARY

The United States Department of Justice (Department or DOJ), Criminal Division (Division), is responsible for, among other mission-essential functions, developing, enforcing, and supervising the application of federal criminal laws. The Docket Case Management System (Docket) will consolidate and modernize the Division's existing master electronic case index and performance management tool, as well as numerous customized Section/Office (Section)-based subsystems, into one Division-wide system. Docket will improve the Division's system infrastructure and provide tools to track and report investigation and prosecution workload for current and future reporting and case management requirements.

This system is in the process of being developed and, once implemented, will be customized to meet the needs of each Section within the Division. The Division is completing this Privacy Impact Assessment (PIA) because Docket may electronically store personally identifiable information (PII) in the form of names of subjects of investigation or defendants, dates of birth, Social Security Numbers (SSNs), citizenship information, law enforcement agency assigned numbers, and investigation information and documents.

Section 1: Description of the Information System

(a) Purpose of the System.

Among its many mission-essential functions, the Division develops, enforces, and supervises the application of all federal criminal laws, except those specifically assigned to other Department entities. The Division and the 93 U.S. Attorneys have the responsibility for overseeing criminal matters as well as certain civil litigation. Division attorneys investigate and prosecute many nationally significant cases. Pursuant to its statutory authorities, the Division has collected and preserved case-related information for many decades.

Docket will replace the Automated Case Management System (ACTS) and the Division Performance Dashboard as the master electronic index, case management tool, and reporting vehicle for certain records maintained by the Division, including case and matter information, memoranda, investigative reports, correspondence to and from the Division, legal papers, evidence, and exhibits.

(b) Operation of System to Achieve Purpose.

Docket is a custom designed web-based database system that: 1) serves as a workspace, by which litigating Sections capture and track information pertaining to investigations and prosecutions that are the sole or shared litigation responsibility of litigating Sections within the Division; 2) maintains detailed information on the status of the case, defendants, charges, sentences, and appeals; 3) manages the internal assignment of cases to attorneys and staff, monitors case progress, and identifies and analyzes workload trends; 4) provides data to support annual budget and special project requests; and 5) serves as a tool to help Sections report key information about workload and activities to

managers within the Division and Department, and occasionally, report to officials and entities outside the Department of Justice (for example, to Congress) concerning the caseload, activities, performance, and Department needs.

Docket will streamline auxiliary systems into a single operating system, allowing Sections to track and report their investigation and prosecution workload in a centralized location. Docket permits customized reporting and record keeping to meet the needs and processes of an individual Section. The Section may store an entire case file in Docket or continue to use its existing file storage system. Finally, Docket will allow data certification and validation, and a Division performance dashboard, described below.

(c) Type of Information Collected, Maintained, Used, or Disseminated.

Docket may contain various forms of PII, either entered into structured data fields or maintained in an unstructured format in documents uploaded to the system. Docket requires a subject's first and last name. A Department of Justice Records Number (DJ#) is automatically generated for each individual case or matter entered into the system.

Other information which may be contained in data fields, based on a Section's need, include:

- Subject or defendant information;
    - Alias
    - Date of Birth
    - Social Security Number
    - Professional Title
    - E-mail Address
    - Phone Number
    - U.S. Marshal's Number
    - Federal Bureau of Prisons' Number
    - Federal Bureau of Prisons' Facility
    - District of Columbia Department of Corrections Number
    - Federal Bureau of Investigation Number
    - Immigration and Naturalization Service Number
    - Immigration Status
    - Immigration Benefit Date
    - Asylee Status
    - Basis of Entry to the U.S.
    - Ethnicity National Group
- Charging, conviction, and sentencing data;
- Investigation and prosecution code name;
- Opening and closing dates for matters;
- Categories describing the type of crime (program categories);
- Assigned employees; and
- Organizations, countries, and/or district courts involved.

Word documents, e-mail messages and their attachments, and other forms of documentation related to an investigation or prosecution may also be uploaded into Docket. The inclusion of this type of case material is based on the Section's needs. In those instances, iterations of the above listed PII may be contained in the uploaded documents. Finally, Docket collects and maintains audit log information from system users to monitor and account for system access and user activity.

(d) Access to the System.

Control over the system is maintained exclusively by the Division. All users must be Division employees or contractors who have successfully completed a background check and mandatory training. The system is maintained on Division servers located in a secure, access-controlled facility, exclusively under the physical control of DOJ. Individuals with access to the Docket are assigned user roles. Each user role has access to specific types of information, based on the minimum access needed for performance of duties. User roles are designated by Section management and implemented in Docket by the Division's Office of Administration. Once access is granted, Docket is only accessible via a government laptop computer after the user's identity is verified through multi-factor authentication.

(e) How Information is Retrieved by the User.

Information is retrieved from Docket by querying most data fields. The standard searches are completed by subject name, defendant name, or the DJ#.

Neither the information contained in uploaded files nor the names of the uploaded files are searchable. De-identified management, statistical, and workload reports can also be run.

(f) Transmission of Information.

Other customized case tracking applications will be migrated into Docket to include:

- ACTS[1]—Contains limited data fields for PII and allows for some tracking of a case through a work-flow.
- Performance Dashboard—Allows the Section to enter data for specified performance metrics regarding its case information.

Information is transmitted out of this system as needed, on a case-by-case basis, by Division employees or contractors.

[1] Information will be migrated to Docket from ACTS for pending cases or cases that were closed after January 1, 2002. Cases closed prior to January 1, 2002, will be transferred to the Records Management Unit for archiving, in accordance with Division policy. New investigations and prosecutions will be manually entered into Docket as they arise.

To the extent that additional transmissions of PII from other applications into Docket is contemplated, the privacy assessment will be re-evaluated and updated as necessary.

(g, h) Size of System; Third Party System.

Docket will be a major, standalone system.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers		
☒ Social Security	☒ Alien Registration	☒ Financial account
☐ Taxpayer ID	☒ Driver's license	☒ Financial transaction
☐ Employee ID	☒ Passport	☐ Patient ID
☒ File/case ID	☐ Credit card	
☒ Other identifying numbers (specify): U.S. Marshall's Service Number, Bureau of Prisons' Register Number, District of Columbia Department of Corrections Number, Federal Bureau of Prisons' Investigation Number, Immigration and Naturalization Service Number.		
The following identifying numbers are most likely to be found in unstructured documents, uploaded into the system: Social Security Numbers, Financial account, Driver's license, Passport, and Financial transaction.		

General personal data		
☒ Name	☒ Date of birth	☐ Religion
☒ Maiden name	☒ Place of birth	☒ Financial information
☒ Alias	☒ Home address	☐ Medical information
☒ Gender	☒ Telephone number	☐ Military service
☒ Age	☒ Email address	☐ Physical characteristics
☒ Race/ethnicity	☐ Education	☐ Mother's maiden name
☒ Other general personal data (specify): Immigration status, Immigration Benefit Date, Asylee Status, Basis for Entry into the U.S., Languages Spoken, Interpreter Requirements		
The following general personal data is mostly like to be found in unstructured documents, uploaded into the system: Maiden Name, Age, Place of birth, Home address, Telephone number, Email address, and Financial information.		
Work-related data		
☒ Occupation	☐ Telephone number	☐ Salary
☒ Job title	☐ Email address	☐ Work history
☒ Work address	☐ Business associates	
☐ Other work-related data (specify):		

The following work-related data is mostly like to be found in unstructured documents, uploaded into the system: Occupation, Job title, and Work address.

Distinguishing features/Biometrics		
☐ Fingerprints	☒ Photos	☐ DNA profiles
☐ Palm prints	☐ Scars, marks, tattoos	☐ Retina/iris scans
☐ Voice recording/signatures	☐ Vascular scan	☐ Dental profile
☐ Other distinguishing features/biometrics (specify):		

System admin/audit data		
☒ User ID	☒ Date/time of access	☒ ID files accessed
☐ IP address	☐ Queries run	☐ Contents of files

Other information (specify)	
☒	Word documents, e-mail messages, attachments, and other forms of electronic documentation related to an investigation or prosecution may also be uploaded into the system. The inclusion of this type of case material is based on the Division's needs. In those instances, iterations of the above listed PII, both checked and unchecked, may be contained in the uploaded documents. The Section's Performance Dashboard will allow Sections to utilize case information to process performance metrics regarding their case information, such as number of matters opened and or closed during the reporting period.

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains		
☒ In person	☒ Hard copy: mail/fax	☒ Online
☐ Telephone	☒ Email	
☒ Other (specify): Information in this system often received via counsel.		

Government sources		
☒ Within the Component	☒ Other DOJ components	☒ Other federal entities
☒ State, local, tribal	☒ Foreign	
☐ Other (specify):		

Non-government sources		
☐ Members of the public	☒ Public media, internet	☒ Private sector
☐ Commercial data brokers		
☐ Other (specify):		

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

Privacy Risk: Over-collection
Mitigation: Because criminal investigations and prosecutions are continually evolving endeavors, it is not always possible to know whether collected information will be relevant or necessary as a matter matures. In order to mitigate these concerns, the Division considered the careful minimization of information collection in the design of Docket. Each Section has a customized interface that solicits the minimal amount of information required to meet that specific Section's needs. Each Section asserting a need for the collection of information such as Social Security Numbers, biological information, and immigration-related information will be discussed and justified.

Privacy Risk: Erroneous or inaccurate information
Mitigation: Based on the sensitive investigative nature of these records, members of the public cannot enter records directly into the system or access it for review. Information in this system is obtained through investigative agencies and prosecutorial or court documents. DOJ has a substantial interest in ensuring the accuracy of the information in this system. Both the investigating agency(ies) and DOJ verify this information as part of the normal procedures associated with day-to-day tasks, which include multiple levels of oversight and review. Every effort is made to diligently review, verify, and correct information from these records. Investigations and prosecutions are conducted in the most timely manner possible based on the variables and complexities of each case. Additionally, the database itself runs validations of the data fields to ensure appropriate forms of information are entered.

For information about the security controls that the Division applied to Docket that assist in mitigating threats related to the collection of PII, please see the responses to questions 6.1 and 6.2, below.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose	
☒ For criminal law enforcement activities	☐ For civil enforcement activities
☐ For intelligence activities	☒ For administrative matters
☒ To conduct analysis concerning subjects of investigative or other interest	☐ To promote information sharing initiatives
☐ To conduct analysis to identify previously unknown areas of note, concern, or pattern.	☐ For administering human resources programs
☒ For litigation	
☐ Other (specify):	

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

Docket will track cases and matters which are presented to and/or pursued by Division attorneys. Docket serves as a day-to-day case management tool, litigation aid, and a review tool. The database, with its online capabilities, permits the Division to compile, maintain, and track the history and status of a case. Initial information is entered into Docket during the case intake and screening stage. Additional information may be added as the matter moves through subsequent investigation and proceedings. In addition to case-by-case tracking, the system allows for the creation of management reports which supports the analysis of workloads and resource needs. This is further described in section 1(b) above.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority	Citation/Reference
☒ Statute	18 U.S.C. § 3001 *et seq.*
☐ Executive Order	
☒ Federal Regulation	28 C.F.R. part 0, subpart K—Criminal Division

☐ Memorandum of Understanding/agreement	
☒ United States Attorney's Manual[2]	Title 9: Criminal
☐ Other (summarize and provide copy of relevant portion)	

3.4 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.)

Disposition of records within Docket will conform to processes and procedures established by the Division Records Management Section (RMS) for the disposition of hardcopy and softcopy records. The records retention schedule for Docket will adopt the retention and disposal criteria to its predecessor system, ACTS, which is covered under N1-060-05-003.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

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. Docket also implements access monitoring, privacy and records controls standardized by the National Institute of Standards and Technology (NIST) Security and Privacy Controls for Federal Information Systems, as defined in 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

[2] https://www.justice.gov/usam/united-states-attorneys-manual.

Modernization Act of 2014 (FISMA).[3] 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 Section provides one-on-one training for employees granted access to Docket. The Division maintains an Account Management Guide and Configuration Management Guide for Docket.

The IT system assessment is documented in the DOJ CSAM 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 investigation, the mere presence of a name in the system can generate the assumption of involvement with criminal 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.

Overall, this particular system is susceptible to the risk that the presence of a name within the system leads to the assumption that that individual is associated with criminal activity. For a list and description of security controls that have been put into place to safeguard against these and other risks, please see the responses to questions 6.1 and 6.2.

[3] Pub. L. 113-283, 128 Stat 3073 (2014).

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared				
	Case-by-case	Bulk transfer	Direct access	Other (specify)	
Within the component	☒	☐	☒	☐	
DOJ components	☒	☐	☐	☐	
Federal entities	☒	☐	☐	☐	
State, local, tribal gov't entities	☒	☐	☐	☐	
Public	☐	☐	☐	☐	
Private sector	☐	☐	☐	☐	
Foreign governments	☒	☐	☐	☐	
Foreign entities	☐	☐	☐	☐	
Other (specify):	☒	☐	☐	☒	Reports to officials outside DOJ (e.g., Congress) concerning Division caseload, activities, performance, and needs.

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

With the exception of de-identified workload, performance, or management reports, this system is designed for internal use. Disclosure of information in this system is extremely limited to the sensitive law enforcement nature of the data it contains. For that reason,

trained, authorized, and supervised Division employees act as the gatekeeper for any releases of information. Case-by-case release of information is performed as required for law enforcement or judicial needs. As described in Section 2.3 above, access controls, annual training, audit logs, role based restriction, extensive security controls, and de-identification practices protect disclosures from this system.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

☒ Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
☐ Yes, notice is provided by other means.	Specify how:
☐ No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

☒ Yes, individuals have the opportunity to decline to provide information.	Specify how: Certain information in the system is not collected directly from the individual, but is submitted by counsel. In certain circumstances and with various consequents, individuals may decline to provide information.
☒ No, individuals do not have the opportunity to decline to provide information.	Specify why not: Certain information is gathered pursuant to investigative means or through the judicial process.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

☐ Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:

☒ No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Use of this information is for investigative or judicial purposes. The necessity to protect the integrity of these processes negates individual consent to use.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Individuals are provided with general notice of the existence of case files through the System of Records Notice, Central Criminal Division Index File and Associated Records, JUSTICE/CRM-001. Generally, individuals are not provided with specific or direct notice of collection about themselves, as it may jeopardize law enforcement investigations or reveal sensitive information such as sources, methods of investigation, or the existence of an investigation. However, in certain circumstances, information in the system is collected directly from counsel on behalf of the individual on whom the record pertains. In certain circumstances and with various consequents, individuals may decline to provide information.

Section 6: Information Security

6.1 Indicate all that apply.

☒ If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:

The Criminal Division uses the Cyber Security Assessment and Management (CSAM) application to manage information system assessments and the Docket Authorization to Operate (ATO). Within CSAM, all databases and information on the General Support System JCON-IIA network are certified and accredited. Docket is currently operating under its ATO signed in August 2017. The expected completion date is approximately August 2018.

☒ A security risk assessment has been conducted.

The security risk assessment is performed as part of the CSAM process and the same answer as provided in 3.2 applies here. All Division IT Systems are subject to the Continuous Diagnostics and Monitoring (CDM) system, which includes constant vulnerability assessment.

☒ Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify:

The Division uses the Cyber Security Assessment and Management (CSAM) application to manage information IT system assessments and the Custom Database Application System Authorization to Operate (ATO). ATOs are granted after a Certification and Accreditation (C&A) has been completed. Docket is currently operating under the Docket ATO signed on 8/17/2018.

☒ Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:

As a Division IT System, Docket system participates in DOJ Continuous Diagnostics and Mitigation (CDM) activities, including annual assessments, penetration tests as required, vulnerability and configuration scans, and is monitored by other means by Division Information Technology Management Security.

☒ Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information:

Audit records include date, timestamps and user IDs of records that are created or altered. Role-based access is defined by multiple methodologies.

☒ Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.

☒ Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.

☒ The following training is required for authorized users to access or receive information in the system:

☒ General information security training

☒ Training specific to the system for authorized users within the Department.

☐ Training specific to the system for authorized users outside of the component.

☐ Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

All Division systems implement technical security to reduce the risk of compromise to PII information. Specifically, certain access and security controls have been utilized to

protect privacy by reducing the risk of unauthorized access and disclosure, including but not limited to the following:

- Docket has a security categorization of FISMA Moderate, and has selected the applicable security controls for a Moderate baseline.
- The system is accessible by DOJ employees and contractors only and utilizes tiered/role based access commensurate with the end-user's official need to access information. Physical access to system servers is controlled through site-specific controls and agreements. Access to this system is granted on a need-to-know basis, based on the principle of least information necessary to perform the job, and is individually verified through the employees PIV card.
- The system is protected by multiple firewalls, an intrusion prevention system, real-time continuous monitoring using malicious code detection and protection, encryption, and other technical controls in accordance with applicable security standards.
- As described throughout this PIA, all Docket users must complete annual CSAT training, as well as read and agree to comply with DOJ information technology Rules of Behavior. Docket system administrators must complete additional professional training, which includes security training.
- Audit logging is configured and logs are maintained to help ensure compliance with tiered/role-based access as well as to help safeguard against unauthorized access, use, and disclosure of information. Audit logs can only be accessed by authorized users with privileged access.

Overall, Docket's defense-in-depth measures are designed to mitigate the likelihood of security breaches and allow the Department time to detect and respond to an attack, thereby reducing and mitigating the consequences of a breach.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.

☒ Yes, and this system is covered by an existing system of records notice.
Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system:

- This system is covered under JUSTICE/CRM-001, Central Criminal Division Index File and Associated Records, last published in full at 72 Fed. Reg. 44182 (Aug. 7, 2007), and amended at 82 Fed. Reg. 24155 (May 25, 2017).

☐ Yes, and a system of records notice is in development.

☐ No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information in this system will be retrieved by the subject's name or the DJ number.