Environment and Natural Resources Division

Privacy Impact Assessment
for the
ENRD JCON System

Issued by:
Joseph Groves
ENRD Senior Component Official for Privacy

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

Date approved: August 5, 2020

Section 1: Executive Summary

The mission of the United States Department of Justice (DOJ), Environment and Natural Resources Division (ENRD), is to enforce the Nation's civil and criminal environmental laws, protect the Nation's natural resources, and handle cases relating to tribal rights and resources. The Division developed the ENRD Justice Consolidated Office Network (ENRD JCON) system to navigate the increasingly complex data requirements associated with enforcing and defending the nation's environmental and natural resource laws and manage the human resource and related personnel information of its workforce. The ENRD JCON system provides the Division's attorneys, managers and support personnel with the ability to collect, organize, analyze, and disseminate information more efficiently. The system maintains various applications that enable ENRD to meet the mission requirements stated above, and includes records related to ENRD employees, internal case management, automated litigation support, FOIA request tracking, financial reporting, administrative personnel services and functions, and information management requests.

ENRD employees – herein defined as ENRD federal staff, detailees, volunteers/interns, and contractors – are the sole users of the ENRD JCON system, and the applications residing on it. A single electronic discovery application is the lone exception to this rule. External user access to the electronic discovery application is granted via a need-to-know/role-based level with tightly controlled privileges. Access to the electronic discovery application by external parties is limited to select government employees, at federal partnering agencies, and expert witnesses under contract with the Division. This access is controlled at the matter level. Not all expert witnesses have security clearances, although ENRD may make that a requirement in the future. External access is not provided to opposing parties, the courts, or the public.

From an infrastructure standpoint, ENRD JCON applications and services are available to the Division's personnel in a hybrid cloud environment which uses a mixture of on-premise and Federal Risk and Authorization Management Program (FedRAMP) compliant government cloud hosting options. Decisions on the selected hosting infrastructure are based on several factors, including: cost, resources, security/access, bandwidth/load, web development, testing, backups, Continuity of Operations (COOP), and administrative maintenance. All infrastructure is aligned with National Institute of Standards and Technology (NIST) security standards and with the Federal Information Technology Acquisition Reform Act (FITARA).

A Privacy Impact Assessment (PIA) has been prepared for the ENRD JCON system because it contains personally identifiable information (PII) about individuals. These individuals include: ENRD employees, in addition to members of the public who are involved in litigation, administrative, and related civil and criminal matters.

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.

ENRD's litigation mission includes civil and criminal enforcement investigations and actions, as well as defensive work on behalf of the United States government.[1] The information collected is used to accomplish activities inherent in the Division's investigations and litigation, including reviewing documents for relevance and privilege claims, tracking use of documentary evidence in litigation, preparing witness kits/binders for depositions and hearings, determining and organizing the facts about the case, and selecting exhibits for trial. Collection, maintenance, and use of the information supports ENRD's litigation and administrative functions.

Furthermore, in addition to being used for carrying out investigations and litigation, ENRD JCON is also used to manage records relating to the ENRD workforce, and includes applications that are used to maintain ENRD personnel files, locator and time keeping information, financial reporting and transit subsidy information, and other records pertaining to the management of ENRD personnel.

ENRD JCON is a standalone major system residing on the DOJ Justice Consolidated Office Network (JCON) general support system platform, which includes a hybrid cloud and on-premise hosting environments. The ENRD JCON system acts as an umbrella for applications necessary to perform ENRD's mission. The system manages administrative processes and interconnects with various applications designed to facilitate ENRD litigation support. These applications include:

- Administrative Service Requests
- Application Lifecycle Management
- Appraisal Management/Requests
- Case Management and Time Reporting
- Comprehensive Human Resource Information
- Correspondence Tracking
- Document Management
- Electronic Discovery Management[2]
- Event Registration
- FOIA Tracking
- Information Management Requests
- MEGA Order & Task Historical Reporting
- Performance Management
- Personnel Locator
- Proposed Consent Decrees

[1] ENRD's mission is to enforce the Nation's civil and criminal environmental laws, including the Clean Air Act, Clean Water Act, and hazardous waste laws. The mission also involves the protection of the Nation's natural resources and handling cases relating to tribal rights and resources. The Division's efforts result in significant public health and other direct benefits to the American people through the reduction of pollution across the Nation and the protection of important natural resources.

[2] In isolated incidents, it is feasible that the unintentional collection of Personally Identifiable Information (PII) data – i.e., listed in the Section 3.1 table – may be temporarily ingested during the electronic discovery management process (**Note:** As part of quality control processes, PII is redacted during the review process). However, aside from the areas specified in the Section 3.1 table, this information is not specifically sought after or collected in a data field housed within the ENRD JCON system.

- Records Management
- Staff Name Change Management
- Superfund Account Management
- Supplemental Application for Financial Analysis and Reporting of Information
- Transit Subsidy Management

For additional information regarding the databases, applications, and tools that have been integrated into the ENRD JCON system, please refer to Appendix A.

As previously stated, ENRD employees are the sole users of the ENRD JCON system, and the applications residing on it. A single electronic discovery application is the lone exception to this rule. External user access to the electronic discovery application is granted via a need-to-know/role-based level with tightly controlled privileges. This application is described more in-depth below.

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

	Authority	Citation/Reference
X	Statute	28 U.S.C. §§ 514-19; 42 U.S.C. § 7413(g); 5 U.S.C. § 552; 42 U.S.C. § 6973(d); 42 U.S.C. § 9622(d)(2); 42 U.S.C. § 9622(i).
	Executive Order	
X	Federal Regulation	28 CFR, Subpart L; 28 CFR § 50.7; 28 C.F.R. § 16.41
X	Agreement, memorandum of understanding, or other documented arrangement	EPA-ENRD MOU, 42 Fed. Reg. 48942-44 (June 15,1977)
X	Other (summarize and provide copy of relevant portion)	Justice Manual 5-12.620 (https://www.justice.gov/jm/justice-manual)

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	Names of DOJ/Component Employees, Contractors and Detailees, and other federal government personnel. Names are collected from members of the public when they make a request for records about themselves, pursuant to the Privacy Act, because they must submit a certification of identity (DOJ form 361).
Date of birth or age	X	A, C, D	Date of birth or age of DOJ Employees and Detailees. Date of birth is collected from members of the public when they make a request for records about themselves, pursuant to the Privacy Act, because they must submit a certification of identity (DOJ form 361).
Place of birth	X	A, C, D	Place of birth or age of DOJ Employees and Detailees.
Gender	X	A	Gender information of DOJ employees and Detailees.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Race, ethnicity or citizenship	X	A, C, D	Race of DOJ employees and Detailees. Citizenship status is collected from members of the public when they make a request for records about themselves, pursuant to the Privacy Act, because they must submit a certification of identity (DOJ form 361).
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, C[3]	Social security numbers (SSNs) of DOJ Employees. **Note:** ENRD minimizes use of SSNs. Select ENRD personnel potentially collect SSNs from members of the public when they make a request for records about themselves, pursuant to the Privacy Act, because they must submit a certification of identity, however, a Privacy Act Notice is included on the form used to collect the information. (DOJ form 361 – **Note:** the SSN field is optional).
Tax Identification Number (TIN)	X	A	Tax identification numbers of expert witness contractors.

[3] **Note:** the SSN field is optional.

(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
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	A, B, C, D	Personal mailing information of DOJ Employees, contractors and Detailees, other federal government personnel, and potentially members of the public (e.g., FOIA request, correspondence to Division, commenting on a Proposed Consent Decree, or from DOJ form 361).
Personal e-mail address	X	A, B, C, D	Personal e-mail addresses of DOJ DOJ Employees, contractors and Detailees, other federal government personnel, and potentially members of the public (e.g., FOIA request, correspondence to Division, commenting on a Proposed Consent Decree, or from DOJ form 361).
Personal phone number	X	A, B, C, D	Personal phone numbers of DOJ Employees, contractors and Detailees, other federal government personnel, and potentially members of the public (e.g., FOIA request, correspondence to Division, commenting on a Proposed Consent Decree, or from DOJ form 361).

(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
Medical records number			
Medical notes or other medical or health information	X	A	Health information of employees is not sought after or collected in a data field housed within the ENRD JCON system. However, printed copies of health information are stored in a restricted access safe. Additionally, select personnel have restricted access to secure folders within the Document Management application, where the following types of files containing health information may be housed: documents provided by employees for purposes of satisfying requirements under the ADAA; EEO settlements; FMLA and sick leave administration; workplace issues arising from pandemics; and select casework.

(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
Financial account information	X	A, C, D	Income information is stored in a database table within the Comprehensive Human Resource Information application. In isolated scenarios select ENRD personnel may collect financial account information for purposes of paying judgments, and settlements from members of the public (US and non-USPERs).
Applicant information	X	A, B, C	Applicant information of DOJ employees and Detailees, other federal government personnel, and potentially members of the public (e.g., information submitted as part of the employment application process).
Education records	X	A, B, C	Education information of DOJ Employees Detailees, and potentially members of the public (e.g., information submitted as part of the employment application process).
Military status or other information	X	A, C	Military information of DOJ employees and Detailees, other federal government personnel, and potentially members of the public (e.g., information submitted as part of the employment application process).

(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 status, history, or similar information	X	A, C	Employment status, history, or similar information of DOJ employees, Detailees, and potentially members of the public (e.g., information submitted as part of the employment application process).
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, C	Employment performance ratings and other performance information of DOJ employees Detailees, and potentially members of the public (e.g., information submitted as part of the employment application process).
Certificates	X	A, C	Certificates of DOJ employees, Detailees, and potentially members of the public (e.g., information submitted as part of the employment application process).
Legal documents	X	A, B, C, D	Legal documents of DOJ Employees, contractors and Detailees, other federal government personnel, and business address of members of the public (US and non-USPERs).
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	A	Web uniform resource locators of DOJ employees and Detailees.
Foreign activities			

(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
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	Environmental Crimes Section collects criminal records information regarding targets and defendants.
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	Several Sections within the Division collect civil law enforcement information, such as civil law violations.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, D	Environmental Crimes and Environmental Enforcement Sections collect whistleblower information.
Grand jury information	X	A, B, C, D	Environmental Crimes Section collects grand jury information.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	Environmental Crimes Section collects information concerning witnesses to criminal matters.
Procurement/contracting records	X	A, B, C	Procurement/contracting records of DOJ Employees, contractors and Detailees, other federal government personnel, and business address of members of the public.
Proprietary or business information	X	A, B, C, D	Business information of DOJ Employees, contractors and Detailees, other federal government personnel, and business addresses of members of the public (US and non-USPERs).

(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
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A	System admin/audit data of DOJ Employees, contractors and Detailees.
- **User ID**	X	A	User ID of DOJ Employees, contractors and Detailees.
- **User passwords/codes**	X	A	User passwords/codes of DOJ Employees, contractors and Detailees.
- **IP address**	X	A	IP addresses of DOJ Employees, contractors and Detailees.
- **Date/time of access**	X	A	Date/time of access of DOJ Employees, contractors and Detailees.
- **Queries run**	X	A	Queries run of DOJ Employees, contractors and Detailees.
- **Content of files accessed/reviewed**	X	A	Content of files accessed/reviewed of DOJ Employees, contractors and Detailees.

(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
- **Contents of files**	X	A	Contents of files of DOJ Employees, contractors and Detailees.
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):					

To ensure National Archives and Records Administration (NARA) and Office of Management and Budget (OMB) electronic records compliance, ENRD is modernizing its information intake efforts. As part of this process, legacy hard copy records are in the process of being converted to electronic files for storage/use. Please see Section 6.3 for additional information regarding records retention and disposition procedures.

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	X
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)	X		
Other (specify): Information exchanges with other federal client agencies (e.g., background investigation process with employees transferring to ENRD, and coordination of trial-related information).					

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

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared*			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Employees within the Division receive restricted access to information as needed, at a role-based permission level. Sensitive information more likely to contain PII, such as law enforcement records, are only accessible to select personnel within the Division.
DOJ Components	X	X		Exported data is used to create a record in DOJ's Consolidated Debt Collection System (CDCS), where the information is stored/maintained. Exported data is used to create a record in DOJ's Unified Financial Management System (UFMS), where the information is stored/maintained. Statistical data reports, GPRA data calls, with PII data excluded.
Federal entities	X			Statistical data reports, with PII data excluded. Compliance Screens from agencies, which contain addresses.

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.**
				Employee Performance Work Plans (PWPs) are manually uploaded into the electronic Official Personnel Folder (eOPF) application.
State, local, tribal gov't entities	X			Environmental Enforcement Section shares information with state or tribal co-plaintiffs on a case-by-case basis. Other ENRD Sections may share information with state, local or tribal governments who are co-parties in litigation, where appropriate.
Public	X			FOIA requests provided to public, with PII data excluded. Press Releases and Proposed Consent Decrees posted to public-facing web presence (i.e., Justice.gov). Select information may be disclosed in public litigation filings, in accordance with DOJ policies.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Select information is shared with counsel, parties, witnesses, and courts or other judicial tribunals for litigation purposes on a case-by-case basis.
Private sector				
Foreign governments	X			On occasion, Environmental Crimes and Environmental Enforcement Sections share information pursuant to treaties with foreign governments.
Foreign entities				
Other (specify):				

* Information sharing agreements will be added to this PIA as they become available.

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.

Proposed Consent Decrees recently submitted by ENRD in the federal district courts, and on which the Division is currently accepting public comments, are available on Justice.gov (https://www.justice.gov/enrd/consent-decrees) and Data.gov (https://catalog.data.gov/dataset/proposed-consent-decrees). As part of quality control processes, the information contained within Proposed Consent Decrees is de-identified prior to release.

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.

Forms related to employment by the Department and ENRD include Privacy Act (e)(3) statements that provide notice to individuals about the collection, use, and sharing of PII required for employment (e.g., background investigations).

The ENRD, DOJ-wide, and government-wide System of Records Notices (SORN) published in the Federal Register provide general notice to the public, which are discussed and referenced in Section 7. If another government agency is involved in the investigation or litigation, the agency's system of records notice would provide notice that the information may be shared with the DOJ for the purpose of a civil or criminal investigation or litigation

For investigations and criminal matters handled by ENRD, individuals are not provided specific notice, but an individual would be notified through applicable court processes as part of the litigation.

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.

Opportunities exist for ENRD employees to optionally provide information associated with their profile in the personnel locator application. Additionally, as part of onboarding procedures ENRD employees are presented with the opportunity to acknowledge a background investigation, including credit check, as part of the process. ENRD employees also provide optional PII via the following forms: SF-181 (Ethnicity and Race Identification); SF-144 (Statement of Prior Federal Service); SF-1152 (Designation of Beneficiary); SF-256 (Self Identification of Disability); DOJ-543 (Employee Locator Form); DOJ-555 (Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act); AD-349 (Employee Address); and state-specific tax withholding forms.

For information related to investigations and litigation matters, opportunities for individuals to participate in the collection, use or dissemination of information must be through court order, warrant, subpoena, discovery requests, voluntary submissions (e.g., Freedom of Information Act (FOIA) or Privacy Act requests/correspondence), and other such legal means. An opposing party may challenge the relevance of the information and not produce the information in litigation, but that challenge would be determined before the information is collected and maintained by the ENRD JCON system. Furthermore, individuals do not have the opportunity to decline to provide information.

Unless individuals are opposing parties in litigation, or voluntarily submit information (e.g., FOIA or Privacy Act requests/correspondence), individuals do not provide information directly to the Division for use in the ENRD JCON system. Individuals who are opposing parties in litigation can object to the Division obtaining the information through the discovery process. Individuals whose information is collected in the course of litigation involving an additional entity, such as another government agency or business, may have the opportunity to consent at the time of collection from the other entity.

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

Individuals seeking to gain access to information within an application housed on the ENRD JCON system, request amendment or correction of their respective information, and/or receive notification of the procedures, may do so by making a FOIA and/or Privacy Act request by following the provisions of those statutes and the Department of Justice regulations on those statutes. Further instructions on how to submit a request are provided on ENRD's FOIA webpage (https://www.justice.gov/enrd/enrd-foia).

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):** 07/28/2020 **If an ATO has not been completed, but is underway, provide status or expected completion date:** n/a **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** The ENRD JCON system recently

	completed its annual assessment of security controls in the Cyber Security Assessment and Management (CSAM) application. A new three year ATO was issued on 07/28/2020, certifying ENRD's ability to maintain Federal Information Processing Standards (FIPS) and FISMA compliant IT systems.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Monitoring functions have been implemented and are conducted on a constant basis at the perimeter of the environment, as well as within the internal network. The system security is tested and evaluated on an annual basis, in support of operational and regulatory requirements.
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:** Auditing functions have been implemented at both the network and application levels. All actions within the environment are continuously tracked and reviewed for unusual activities. ENRD's Office of Information Technology (OIT) utilizes automated log collection, aggregation, reporting and alerting tools in order to more efficiently review security and audit logs. These tools highlight and alert issues to appropriate ENRD OIT personnel in real-time. Additionally, manual log reviews are performed ad hoc based on any suspicious behavior or events that may require further investigation. ENRD retains system and security logs according to NIST standards.
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:** There is no additional training specific to the ENRD JCON system. All ENRD personnel are annually required to complete the DOJ's Office of Privacy and Civil Liberties (OPCL) mandatory privacy training course via LearnDOJ.

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?

The ENRD JCON system security plan, including administrative and technological controls, is documented in accordance with DOJ guidance, policies and directives. The system exists on a physically secure, environmentally protected, DOJ network protected by firewalls, and is administered by DOJ/ENRD contractors. All privileged system administrator functions are performed by DOJ/ENRD federal employees. Non-privileged administrative functions (e.g., PC/Laptop installs,

printer maintenance, mobile device troubleshooting, etc.) are performed by DOJ/ENRD contractors who have the appropriate clearance. The system's connection to the JCON network and the outside world is protected by firewalls, constantly monitored via intrusion detection software, and housed in a secure location with physical access controls. Firewall and operating system security are tested monthly. Patches are applied as appropriate to maintain system security. System access is monitored by inspection of event logs, system logs, web logs, database application logs, and firewall logs.

Access to the ENRD JCON system is only granted to DOJ/ENRD federal employees and fully cleared DOJ/ENRD Contractors. All DOJ/ENRD federal employees and DOJ/ENRD contractors are required to sign the same confidentiality agreement and system rules of behavior. Access to specific databases/folders/materials is granted on a need-to-know basis requiring a user account and password. All ENRD JCON accounts are "named user" accounts assigned to a single individual and require PIV authentication. A documented process exists for requesting, granting, and reviewing account activity, and terminating accounts. Test, training, or temporary accounts are not permitted in order to accurately log the individual accessing the information.

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.)

Files managed on the ENRD JCON system may include both federal records and non-records that are associated with a wide-array of litigation case files. The retention policies for the files depend on the federal record status as well as the classification of the type of case file to which the files pertain. The DOJ record retention schedules are published at Archives.gov (https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060).

Record retentions for case files range from approximately 5 years to 65 years after the case closure date. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of NARA. Paper and electronic non-records are destroyed when no longer needed.

In accordance with the Federal Records Act, DOJ's Office of Records Management Policy (ORMP), and consistent with NARA standards, ENRD ensures that all applications hosted on the ENRD JCON system are in compliance with appropriate retention schedules to manage the use, maintenance, retention, and disposition of DOJ records created and captured. A list of the relevant records retention schedules is included in Appendix A.

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:*** A new SORN is required for ENRD JCON. However, in the meantime, the SORNs listed below cover the applications within the network:

Records pertaining to ENRD cases and files are covered by:

- DOJ/ENRD-003, *Environment & Natural Resources Division Case & Related Files System*, 65 FR 8990 (Feb. 23, 2000) (as amended); https://www.govinfo.gov/content/pkg/FR-2000-02-23/pdf/00-3116.pdf.

Records pertaining to maintenance of DOJ networks and computers are covered by:

- DOJ-001, *Accounting Systems for the Department of Justice*, 69 FR 31406 (June 3, 2004) (as amended), https://www.govinfo.gov/content/pkg/FR-2004-06-03/pdf/04-12578.pdf.

Records pertaining to FOIA/PA requests are covered by:

- DOJ-004, *Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records*, 77 FR 26580 (May 4, 2012) (as amended), https://www.govinfo.gov/content/pkg/FR-2012-05-04/pdf/2012-10740.pdf.

Records pertaining to personnel records and files are covered by:

- DOJ-009, *Emergency Contact Systems for the Department of Justice*, 69 FR 1762 (Jan. 12, 2004) (as amended), https://www.govinfo.gov/content/pkg/FR-2004-01-12/pdf/04-583.pdf.

- DOJ-014, *Department of Justice Employee Directory Systems*, 74 FR 57194 (Nov. 4, 2009) (as amended), https://www.govinfo.gov/content/pkg/FR-2009-11-04/pdf/E9-26526.pdf.

- OPM/GOVT-1, *General Personnel Records*, 77 FR 79694 (Dec. 11, 2012) (as amended), https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf.

- OPM/GOVT-2, *Employee Performance File System Records*, 71 FR 35347 (June 19, 2006) (as amended), https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf.

Section 8: Privacy Risks and Mitigation

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

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the Department's official duties is always a potential threat to privacy. ENRD mitigates this risk through implementation of data access controls to ENRD JCON. Furthermore, information is given only to those individuals

who require access to perform official duties. There are no outside users who are permitted access to the ENRD JCON system, including personnel from the larger DOJ community. The ENRD JCON system collects only the data which is required to complete the tasks at hand. When an ENRD employee departs from the Division, appropriate measures are taken to deactivate the user access and accounts to ENRD information.

Access to SSNs is restricted and only available to certain users with a need to know, for administrative purposes. SSNs are not viewable outside of users who are permitted access in order to perform key administrative functions. SSNs stored in ENRD JCON applications are encrypted, and the Division continues to seek alternative methods to avoid the use of SSNs.

b. Potential Threats Related to Use of the Information

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

ENRD mitigates these risks by requiring all ENRD employees to annually complete the DOJ Cybersecurity Awareness Training (CSAT), and the DOJ OPCL Privacy Training. Additionally, ENRD personnel are required to review and acknowledge the application of the ENRD Rules of Behavior before being granted access to the ENRD JCON system. Users are reminded to use care when communicating with employees from other Government agencies, outside counsel, opposing parties, and expert witnesses.

c. Potential Threats Related to Dissemination

There is a potential risk to privacy that could result from improper access and the potential unauthorized disclosure of the information within the ENRD JCON system. However, security protections that authorize and limit a user's access to information within the system mitigate this risk.

ENRD mitigates this risk by using the DOJ Identity Management solutions, controlling access to information on a need to know basis, and providing adequate training in the proper use of the ENRD JCON system. As roles change or users move to new ENRD teams, accesses are adjusted and removed to reflect the changes in roles and responsibilities. Usage patterns are tracked and reviewed for anomalous behavior. Users are granted access to only the information applicable to their role. Procedures to terminate access to the ENRD JCON system are promptly implemented – when an ENRD employee departs/exits/retires – by ENRD OIT, and the Justice Management Division (JMD) Office of the Chief Information Officer (OCIO).

On a Department-wide level, ENRD's security defenses are shared with DOJ Justice Security Operations Center (JSOC) to ensure appropriate perimeter control and data content monitoring. Security Defenses are augmented by solutions deployed within the ENRD JCON system, including additional firewalls and monitoring tools.

Appendix A

The following is an overview of databases, applications, and tools hosted on the ENRD JCON system. Additionally, relevant records retention schedules are provided.

Name	Description	Records Schedule
Administrative Service Requests	Help Desk solution to request and track building service related requests.	• DAA-GRS-2016-0011-0009
Application Lifecycle Management	One-stop solution to manage all phases of design, development, testing, deployment, and maintenance in the Development, Security, and Operations (DevSecOps) arena.	The application is still in the development stage. ENRD will continue to work with records and information management personnel to identify the applicable records retention schedule.
Appraisal Management/Requests	Plans and tracks appraisal review and interest calculation requests.	• N1-060-09-13
Case Management and Time Reporting	One-stop case management solution. Encompasses time tracking module for ENRD attorneys, paralegals, and other specified employees to accurately report time spent on cases and other activities.	• N1-060-05-06
Comprehensive Human Resource Information	One-stop solution for collecting, tracking, managing, and reporting ENRD personnel information.	• N1-060-09-21
Correspondence Tracking	An automated log that tracks the routing and status of ENRD correspondence packages.	• DAA-GRS-2013-0002-0016
Document Management	Primary repository for documents created in ENRD, and received from other sources, in carrying out	• DAA-GRS-2013-0002-0007 • DAA-GRS-2013-0002-0008

Name	Description	Records Schedule
	ENRD business.	
Electronic Discovery Management	ENRD's litigation support processes align with the Electronic Discovery Reference Model (EDRM): Identify, Preserve, Collect, Process, Review, Analyze, Produce, and Present. The EDRM necessitates an integrated suite of tools to facilitate a one-stop solution for managing/providing: support requests (OPUS), case assessment, fact management, review, production, analytics, and legal hold functionalities.	The application is still in the development stage. ENRD will continue to work with records and information management personnel to identify the applicable records retention schedule.
Event Registration	One-stop solution for creating, sending, and managing internal events.	The application is still in the development stage. ENRD will continue to work with records and information management personnel to identify the applicable records retention schedule.
FOIA Tracking	Tracks receipt and processing of Freedom of Information Act (FOIA) requests.	• DAA-GRS-2019-0001-0002
Information Management Requests	Help Desk solution to request and track information management related service requests.	The application is still in the development stage. ENRD will continue to work with records and information management personnel to identify the applicable records retention schedule.
MEGA Order & Task Historical Reporting	Creates, organizes and maintains MEGA Contract Task order documentation and financing.	• DAA-GRS-2013-0003-0001

Name	Description	Records Schedule
Performance Management	One-stop solution for employees to receive, and for supervisors to issue, work plans, progress reviews, and performance evaluations.	• N1-060-09-21
Personnel Locator	Centralized, searchable directory of employee expertise with associated locator information to facilitate professional contacts. Employees also have the option to add emergency contact information.	• N1-060-08-21
Proposed Consent Decrees	Consent decrees that the Division has recently lodged in the federal district courts and on which the Division is currently accepting public comment.	The application is still in the development stage. ENRD will continue to work with records and information management personnel to identify the applicable records retention schedule.
Records Management	Tracking solution for official personnel files.	• DAA-GRS-2013-0002-0016
Staff Name Change Management	Self-service solution to request change in legal name in all ENRD web applications, including: payroll, benefits, personnel records, JCON addresses, PIV Cards, transit subsidies, parking passes, CMS time reporting, and credit/procurement cards as appropriate.	• DAA-GRS-2017-0007-0001
Superfund Account Management	Accounting and program management tools to automate the process of tracking and calculating	The application is still in the development stage. ENRD will continue to work with records and information

Name	Description	Records Schedule
	billable and/or recoverable expenses related to the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA).	management personnel to identify the applicable records retention schedule.
Supplemental Application for Financial Analysis and Reporting of Information	Expert contracts management, with a query-and-report tool on expert witness and litigation consultant contract information.	• DAA-GRS-2013-0003-0001
Transit Subsidy Management	Submit and track transit subsidy applications for the National Capital Region, as well as Field locations.	• DAA-GRS-2016-0015-0018