Civil Division

Privacy Impact Assessment
for
Civil Division Justice Consolidated Office Network (CIV-JCON)

Issued by:
Kenneth Hendricks, Senior Component Official for Privacy

Approved by: Hannah Mayer
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: March 20, 2025

(May 2022 DOJ PIA Template)

Section 1: Executive Summary

The Civil Division Justice Consolidated Office Network (CIV-JCON) General Support System is the primary automated information system of the Department of Justice's Civil Division. It provides an automated litigation environment to support the management of cases for the attorneys and staff members of the Civil Division.

Pursuant to the privacy provisions of the E-Government Act of 2002, Civil Division has prepared a Privacy Impact Assessment (PIA) for this system because it collects, maintains, and disseminates information in identifiable form. CIV-JCON hosts a variety of personally identifiable information (PII), including names, personal identifiers, contact information, and case numbers for employees, contractors, job applicants, Privacy Act (PA) and Freedom of Information Act (FOIA) requestors, and individuals involved in Division litigation.

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.

The CIV-JCON system is designed to offer a wide range of services and products that help attorneys and other professional staff members acquire, organize, analyze, and present evidence. Through the use of individual workstations and servers the system provides users access to office automation applications such as an electronic mail system, computer data processing, document management, trial presentation systems, Internet access to the U.S. Courts, Westlaw, Office of Personnel Management (OPM) systems for functions related to human resources (e.g., USAJOBS and the electronic Official Personnel Folder (eOPF), as well as other technologies (e.g., Cherwell ticketing system for IT Service Management and VMWARE Airwatch for mobile device management). The system effectively organizes litigation materials so that the litigating attorneys and other professional staff can rapidly locate information and make the best use of it in conducting a lawsuit or settlement negotiations. Appendix A to this document includes a list of applications and tools hosted on the CIV-JCON system.

CIV-JCON provides a dynamic flexible system with infrastructure consisting of a robust network framework and physical and virtualized server platforms with a scalable storage system designed to ensure data integrity. It uses virtualized workstations and applications to deliver a secure environment necessary to support the Civil Division's need for support of its varied litigation cases.

Civil Division also stores and processes FOIA/PA records in the CIV-JCON document management folders and in the Civil Online Relativity Application (CORA). Civil Division also transmits FOIA/PA records via email.

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	5 U.S.C. § 301 (agency operations); 28 U.S.C. §§ 514-19.
Executive Order	
Federal regulation	28 C.F.R. §§ 0.45-0.49.
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
Name	*X*	A, B, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records, which might contain listed PII. Other Federal Government and CIV personnel listed PII are collected during case collaboration, or for system administration and audit activities.
Date of birth or age	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records, which might contain listed PII.
Place of birth	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records, which might contain listed PII.
Sex	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records, which might contain listed PII.
Race, ethnicity, or citizenship	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Religion	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Social Security Number (full, last 4 digits or otherwise truncated)	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Tax Identification Number (TIN)	*X*	C, D	The system may host case-related files and FOIA/PA records which might contain listed PII.

(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	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. Some applications on the system may host case-related files and FOIA/PA records which might contain listed PII.
Alien registration number	*X*	A, C, D	Some applications on the system may host case-related files and FOIA/PA records which might contain listed PII.
Passport number	*X*	A, C, D	The system may host case-related files and FOIA/PA records which might contain listed PII.
Mother's maiden name	*X*	C, D	The system may host case-related files which might contain listed PII.
Vehicle identifiers	*X*	A, C, D	The system may host case-related files and FOIA/PA records which might contain listed PII. Parking-related data for CIV employees.
Personal mailing address	*X*	A, B, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII. Other Federal Government and CIV personnel listed PII are collected during case collaboration, or for system administration and audit activities.
Personal e-mail address	*X*	A, B, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII. Other Federal Government and CIV personnel listed PII are collected during case collaboration, or for system administration and audit activities.
Personal phone number	*X*	A, B, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII. Other Federal Government and CIV personnel listed PII are collected during case collaboration, or for system administration and audit 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
Medical records number	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Medical notes or other medical or health information	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Financial account information	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Applicant information	*X*	A, C	System users access HR personnel data, which can include this PII.
Education records	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Military status or other information	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Employment status, history, or similar information	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Employment performance ratings or other performance information, e.g., performance improvement plan	*X*	A, C, D	JCON system users access HR personnel data which include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Certificates			

(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
Legal documents	*X*	C	JCON system users access HR personnel data which may include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Device identifiers, e.g., mobile devices	*X*	A	CIV-JCON system uses VMWARE Airwatch to manage Civil Division-issued mobile devices.
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	*X*	C, D	HR personnel may include the listed form of PII. The system may host case-related files and FOIA/PA records which might contain listed PII.
Juvenile criminal records information	*X*	C, D	The system may host case-related files and FOIA/PA records which might contain listed PII.
Civil law enforcement information, e.g., allegations of civil law violations	*X*	C, D	The system may host case-related files and FOIA/PA records which might contain listed PII.
Whistleblower, e.g., tip, complaint, or referral	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
Grand jury information	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
Procurement/contracting records	*X*	A, B, C	Cherwell ticketing system stores government and contractor record information.
Proprietary or business information	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.

(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
- **Video containing biometric data**			
- **Fingerprints**	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**	*X*	C	The system may host case-related files and FOIA/PA records which might contain listed PII.
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analysis. Other Federal Government personnel listed PII are collected during case collaboration
- **User ID**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analyzing. Other Federal Government personnel listed PII are collected during case collaboration
- **User passwords/codes**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analyzing. Other Federal Government personnel listed PII are collected during case collaboration
- **IP address**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analysis. Other Federal Government personnel listed PII are collected during case collaboration.
- **Date/time of access**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analyzing. Other Federal Government personnel listed PII are collected during case collaboration.

(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
- **Queries run**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analysis. Other Federal Government personnel listed PII are collected during case collaboration.
- **Contents of files**	*X*	A, B	System admin audit data is stored on Windows domain controller. Splunk also collects this data for analysis. Other Federal Government personnel listed PII are collected during case collaboration.
Other (please list the type of info and describe as completely as possible):	*X*	A, B, C, D	Because of the varied nature of the records relevant to the various CIV activities performed via the system, other types of PII not listed above may be collected, maintained, or disseminated.

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		Online	*X*
Phone	*X*	Email	*X*		
Other (specify):					

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

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
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*	Department of Justice employees and contractors with assigned roles and permissions can only access information by logging into CIV-JCON system.
DOJ Components			*X*	Department of Justice employees and contractors with assigned roles and permissions can only access information by logging into CIV-JCON system.
Federal entities	*X*		*X*	In some instances, the Civil Division may make case-by-case transmittals to OPM or to benefits management contractors. Other Federal Government personnel are given access to CIV-JCON system during case collaboration.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				

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.**
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.

CIV-JCON does not release information for "Open Data" purposes. If a specific application on CIV-JCON were to be a source of information for "Open Data" purposes, CIV would address that in the relevant application's Initial Privacy Assessment (IPA).

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.

Generalized notice to the public is provided by the SORNs listed in section 7.2. Privacy Act Statements are provided where appropriate when information is collected directly from individuals and saved in a System of Records.

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.

In some Civil Division cases, the collection of PII is incidental and not collected directly from an individual. In other cases, PII is collected from an individual pursuant to rules of discovery. The investigation or discovery process typically does not allow the type of voluntary participation contemplated in this question due to the need to maintain the integrity of the information responsive to the discovery process.

In other contexts, individuals submit PII to the Civil Division on employment applications and related forms, or in Privacy Act requests. Privacy Act Statements are provided where appropriate that indicate whether the collection of information is voluntary.

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 and their representatives can request access to information under the Freedom of Information Act or the Privacy Act by submitting requests directly to the Civil Division (see https://www.justice.gov/civil/foia for submission information). An individual can submit a Privacy Act Amendment or Correction request of their first-party information (see https://www.justice.gov/opcl/doj-privacy-act-requests for submission information).

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):** Granted: March 12, 2021 Expires: May 15, 2025 **If an ATO has not been completed, but is underway, provide status or expected completion date:** **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:** CIV-JCON is categorized as a moderate system based on a review of the aggregate impact of a loss of confidentiality, integrity, and availability of the information contained within it.
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**

	CIV-JCON operates within the boundary of the Civil Division and is subject to full system monitoring and auditing in accordance with the Department of Justice guidelines. System documentation supporting these activities are maintained within the department's system of records, Joint Cybersecurity Assessment & Management (JCAM) tool.
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:** System logs are captured in Splunk, reviewed bi-weekly and stored in SharePoint.
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**. All contractors granted access to CIV-JCON are required to sign the DOJ General and/or Privileged Rules of Behavior, as determined by their role. They are also required to complete the OPCL privacy training module on LearnDOJ.
	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:

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?

Administrative Controls: Authorized users are assigned a role that gives them data access on a need-to-know basis to accomplish their duties. A user's access to CIV-JCON is ended within twenty-four hours of termination from the JCON Network. Additionally, each CIV-JCON user is part of Justice Consolidated Office Network (JCON). JCON requires each user to attend Civil Division's Computer Security Awareness Training (CSAT) to continue to bring more awareness to each user's responsibility in protecting personally identifiable information. At the end of the annual training, the users are required to sign the Rules of Behavior (ROB) that outlines each user's responsibility in safeguarding personally identifiable information (PII).

Technical Controls: Access to truncate SSN data is restricted to user roles that require that data. BitLocker is utilized to encrypt data at rest and SSL is used to encrypt data in transit. Active directory security groups and NTFS permission on the file shares are used to make sure only authorized personnel have access to related data.

Physical Security: The buildings that host CIV-JCON servers are manned by security guards 24/7, who allow building access to authorized personnel only. The server rooms in the buildings are secured by PIV card reader security and only authorized users with a

valid PIV card can access them. Access to all server rooms is logged and monitored by JCON. All the data collected are stored in Civil Division's data center under the control of the Chief Information Officer's (CIO) office and has neither public interface nor access beyond Civil Division employees and contractors.

Database access is limited to a handful of Civil Division employees and contractors who have administrative access to the database servers. These employees and contractors require a special administrative PIV card to access the database directly. Each administrative user undergoes separate annual Rules of Behavior (ROB) training and is required to sign a rules and responsibility acknowledgement in safeguarding the CIV-JCON data.

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.)

Record retention policies depend on the federal record status and the classification of the type of case file. Retention periods for case files range from approximately 5 years to permanent. Temporary records are destroyed at the end of the retention period, and permanent records are transferred to the custody of the National Archives and Records Administration at intervals noted in the records retention schedules. Non-records, such as duplicates and unnecessary discovery or other submitted documents, are destroyed when no longer needed for convenience of reference. The Department of Justice record retention schedules are published at: https://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-justice/rg-0060.

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:

The following SORNs are available at: https://www.justice.gov/opcl/doj-systems-records.

- DOJ-002, Department Computer Systems Activity and Access Records, last published in full at 64 Fed. Reg. 73585 (Dec.30, 1999) and amended at 82 Fed. Reg. 24147 (May 25, 2017).
- DOJ-004, Freedom of Information Act, Privacy Act, and Mandatory Declassification Review Records, last published in full at 77 Fed. Reg. 26580 (May 4, 2012), and amended at 82 Fed. Reg. (May 25, 2017).
- DOJ-014, Department of Justice Employee Directory System, last published in full at 74 Fed. Reg. 57194 (Nov. 4, 2009) and amended at 82 Fed. Reg. (May 25, 2017).
- CIV-001, Civil Division Case File System, 63 Fed. Reg. 8659-8665 (Feb. 20, 1998), as amended at 82 Fed. Reg. 24147 (May 25, 2017).

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. CIV mitigates this risk through implementation of data access controls to CIV-JCON. Furthermore, information is given only to those individuals who require access to perform official duties. The CIV-JCON system collects only the data which is required to complete the tasks at hand. When an CIV employee departs from the Division, appropriate measures are taken to deactivate the user access and accounts to CIV information.

Each JCON user is required to attend Civil Division Computer Security Awareness Training (CSAT), to bring awareness to user's responsibility in protecting personally identifiable information. In addition, each new CIV employee must complete the OPCL privacy training module on LearnDOJ.

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 CIV-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.

BitLocker is utilized to encrypt SSN data at rest and SSL is used to encrypt SSN data in transit. Active directory security groups and NTFS permission on the file shares are used to make sure only authorized personnel have access to SSN-related data. Additionally, database access is limited to a handful of Civil Division employees and contractors who have administrative access to the database servers. These employees and contractors

require a special administrative PIV card to access the database directly.

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 CIV-JCON system. However, security protections that authorize and limit a user's access to information within the system mitigate this risk.

Authorized users, including users from other DOJ components and Federal government agencies, are assigned a role that gives them data access on a need-to-know basis to accomplish their duties. A user's access to CIV-JCON is ended within twenty-four hours of termination from the JCON Network.