Justice Management Division

Privacy Impact Assessment
for the
Justice Web Interface to the National Criminal Information Center (NCIC) (JWIN)

Issued by:
Morton J. Posner
JMD General Counsel and Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director, Office of Privacy and Civil Liberties (Acting)
U.S. Department of Justice

Date approved: August 2, 2023

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Department of Justice (DOJ) is responsible for maintaining criminal justice information and assuring that the criminal history information it maintains, wherever it appears, is collected, stored, and disseminated in a manner to ensure the accuracy, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in any agency determination about an individual, to ensure the reliability, integrity, and security of such information, and to protect individual privacy.

To achieve this purpose, the U.S. Department of Justice, Justice Management Division (JMD), Service Delivery Staff (SDS), Law Enforcement Services & Information Sharing (LESIS), developed the Justice Web Interface to NCIC (JWIN) system, the successor information system to the Justice Telecommunications System (JUST).[1] JWIN is not a repository, but securely connects Federal and Tribal Agencies in criminal justice and law enforcement communities to criminal justice information. JWIN is a web user interface that authorized users may log into to access information they are authorized to view. The FBI's Criminal Justice Information Services (CJIS) Division maintains criminal justice information through the National Crime Information Center (NCIC)[2], Next Generation Identification (NGI) via Interstate Identification Index (III), and National Instant Criminal Background Check System (NICS). JWIN also securely connects to the International Justice and Public Safety Network (Nlets) which serves as interstate justice/public safety network for the exchange of law enforcement, criminal justice, and public safety information.[3] JWIN's primary function is to act as a store-and-forward message switch that provides DOJ, other Federal agencies, non-DOJ agencies, and the Tribal Access Program for National Crime Information (TAP) with access to Criminal Justice Information (CJI) stored in various DOJ law enforcement databases.

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.

JWIN is a message switch (which allows for the querying and updating of information, such as criminal histories) that provides authorized user agencies access to state and national criminal justice

---

[1] *See* Justice Management Division, Initial Privacy Assessment OPCL No. 16-936, Justice Telecommunications System (JUST) (Feb. 13, 2017).
[2] NCIC data is hosted by the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS). *See* Federal Bureau of Investigation, Privacy Impact Assessment, National Crime Information Center (NCIC) (Nov. 7, 2022), https://www.fbi.gov/file-repository/pia-ncic-020723.pdf/view.
[3] Nlets is a private not for profit corporation that manages an interstate justice/public safety network for the exchange of law enforcement, criminal justice, and public safety information. https://www.nlets.org/.

information systems, such as NCIC, III, NICS and Nlets. JWIN provides user-based access as well as system-to-system interconnections. User access is provided through a web-based portal that allows authorized user agencies to enter, modify and query records in NCIC, query and modify records in III and NICS, and query records in Nlets. NCIC, III, NICS, and Nlets provides and maintains state and national criminal justice information from participating agencies relating to criminal justice and national security missions. These national databases include an extensive collection of criminal justice information that can be accessed electronically by, and furnished to, any authorized user agency without the need for manual processing.

JWIN maintains data logs for audit and administrative purposes, and these logs are accessible to the DOJ Criminal Justice Information Services (CJIS) Systems Agency (CSA) during the audit cycle for User Agencies and individual users. Authorized users are determined by the User Agency's Terminal Agency Coordinator (TAC) and governed by the User Agency MOU; all TAC responsibilities are outline in the UA MOU. Authorized users are required to complete all required NCIC Certification Training and Examination. The NCIC Certification exam is synced to the JWIN users account and will automatically disable access for a user who has not completed their NCIC Certification, or their certification has expired.

JWIN supports these DOJ mission essential services:

- Protect the United States from terrorist attacks and foreign intelligence operations and espionage; share law enforcement information related to these matters; investigate/prosecute terrorists, foreign agents, and organizations that threaten the United States.
- Conduct federal law enforcement activities and coordinate federal law enforcement response as needed in national and international emergencies.
- Operate the federal detention and prison systems to ensure the continued confinement of prisoners.
- Equip the Department's law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties**.**

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	31 U.S.C. Part 501; 28 U.S. Code § 534; 28, Code of Federal Regulations, Part 20, Criminal Justice Information Systems.
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs	(4) Comments
Name	X	A, B, C, and D	Names of DOJ employees and contractors, other Federal government personnel, members of the public (both USPERs and non-USPERs)
Date of birth or age	X	C and D	Dates of birth on members of the public (both USPERs and non-USPERs)
Place of birth	X	C and D	Places of birth of members of the public (both USPERs and non-USPERs)
Gender	X	C and D	Gender of members of the public (both USPERs and non-USPERs)
Race, ethnicity, or citizenship	X	C and D	Race, ethnicity, or citizenship of members of the public (both USPERs and non-USPERs)
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C and D	Full Social Security Numbers are collected
Tax Identification Number (TIN)	X	C and D	Tax Identification Number (TIN) of members of the public (both USPERs 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
Driver's license	X	C and D	Driver's license of members of the public (both USPERs and non-USPERs)
Alien registration number	X	C and D	Alien registration number of members of the public (both USPERs and non-USPERs)
Passport number	X	C and D	Passport number of members of the public (both USPERs and non-USPERs)
Mother's maiden name	X	C and D	Mother's maiden name of members of the public (both USPERs and non-USPERs)
Vehicle identifiers	X	C and D	Vehicle identifiers of members of the public (both USPERs and non-USPERs)
Personal mailing address	X	C, and D	Personal mailing address of members of the public (both USPERs and non-USPERs)
Personal e-mail address	X	C, and D	Personal e-mail address of members of the public (both USPERs and non-USPERs)
Personal phone number	X	C and D	Personal phone number is collected from DOJ and other Federal users for account management, and from members of the public (US PERs and non-US PERs) for criminal justice purposes.
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			

(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
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices	X	C and D	Cell phone numbers of members of the public (both USPERs and non-USPERs)
Web uniform resource locator(s)			
Foreign activities	X	C and D	Criminal records queries may contain foreign activities on members of the public (both USPERs and non-USPERs).
Criminal records information, e.g., criminal history, arrests, criminal charges	X	C and D	Criminal records information, e.g., criminal history, arrests, criminal charges of members of the public (both USPERs and non-USPERs)
Juvenile criminal records information	X	C and D	Juvenile criminal records information of members of the public (both USPERs and non-USPERs)
Civil law enforcement information, e.g., allegations of civil law violations	X	C and D	Civil law enforcement information, e.g., allegations of civil law violations members of the public (both USPERs and non-USPERs)
Whistleblower, e.g., tip, complaint, or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			

(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
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**	X	C and D	Photographs or photographic identifiers of members of the public (both USPERs and non-USPERs)
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	C and D	Scars, marks, tattoos of members of the public (both USPERs and non-USPERs)
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users

(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
- **User passwords/codes**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users
- **IP address**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users
- **Date/time of access**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users

(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 and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users
- **Content of files accessed/reviewed**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users
- **Contents of files**	X	A, B and C	User ID of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel and Members of the Public – US Citizens or Lawful Permanent Residents (USPERs) which include Tribal Users

(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
Other (please list the type of info and describe as completely as possible):	X	C and D	JWIN contains an unrestricted text field that allows users to enter any information, whether or not identified above. Additionally, JWIN contains fields to capture security clearances and Trusted Traveler Programs; Universal Control Number (UCN) – a unique identifier assigned to each fingerprint submitted to FBI CJIS; State Identification Number (SID) - identifies persons in the III database.

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

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

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
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): The primary source of information is data collected by Federal and Tribal agencies. This information collected may include information that was initially collected from other entities, such as NCIC. JWIN access to Interpol data sources and the Nlets connection provides access to Canadian law enforcement information sources.					

Non-government sources:

Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): The primary source of information is data collected by Federal and Tribal agencies. This information collected may include information that was initially collected from other entities, such as Nlets.					

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.

JWIN authorized users are individual persons granted access, based on their legal authority. The legal authority for authorized users is determined by the user agency accessing JWIN. Authorized users access data with their unique JWIN user account. Any data queried and updated must be used for the purpose provided during the query or entry and fall within the approved authorities. The DOJ CSA is responsible to ensure User Agency and individual user adherence to applicable statutes, regulations, and policies, as they pertain to the use of and access to CJI and Criminal History Record Information (CHRI) through DOJ [CJIS?]. The DOJ CSA's Audit Cycle is every three years and follows the Federal fiscal year, which begins on October 1 and ends on September 30. JWIN Administrators work with User Agency POCs on account management to ensure access is terminated once authorized users no longer have a need to access the system. JWIN also has system interconnections with CJI Systems at FBI CJIS and State Systems that allow records to be queried and updated.

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	Authorized JMD personnel can login to JWIN for the purpose of supporting users, conducting audits, troubleshooting issues, and other support-related duties.
DOJ Components		X	X	Authorized users within DOJ Components can login to JWIN (or leverage a system interconnection) to query or update records stored in national crime information systems, such as NCIC or Nlets.

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.**
				ATF to JWIN bulk request for Gun checks.
Federal entities			X	Authorized users within Federal entities including DOJ can login to JWIN to query or update records stored in national crime information systems, such as NCIC or Nlets.
State, local, tribal gov't entities		X	X	Authorized users within tribal government entities can login to JWIN to query or update records stored in national crime information systems, such as NCIC or Nlets. Tribe and Territory Sex Offender Registry System (TTSORS) bulk transfer of NCIC record updates.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes			X	Authorized users within courts can login to JWIN to query or update records stored in national crime information systems, such as NCIC or Nlets. Court personnel may also receive criminal justice information from authorized users.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

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

Information from JWIN will *not* be released to the public for "Open Data" purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Individuals have been notified that the account, audit log, and user records maintained in this system for the purpose of monitoring system activity are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" 86 FR 37188 (July 14, 2021). Individuals have also been notified that the criminal justice information retrieved utilizing identifying particulars by Federal criminal justice entities for the purposes of providing a computerized database of NCIC files is covered by JUSTICE/FBI-001, "National Crime Information Center (NCIC)" 64 FR 52343 (Sept. 28 1999); 66 FR 8425 (Jan. 31, 2001); 72 FR 3410 (Jan. 25, 2007) (rescinded by 82 FR 24147); 82 FR 24147 (May 25, 2017); 84 FR 47533 (Sept. 10, 2019).

In addition, to the extent that information is collected directly from individuals, a Privacy Act (e)(3) statement is provided at the point of collection.

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.

JWIN is not an information system repository and therefore cannot provide for the voluntary collection, use, or dissemination of information in the system. Any opportunities for individuals to voluntarily participate in the collection, use or dissemination of information stored in systems connected to JWIN are handled by said systems, such as NCIC or Nlets.

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 have been notified that the account, audit log, and user records maintained in JWIN for the purpose of monitoring system activity can be accessed or amended, in accordance with DOJ regulations, and in accordance with JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" 86 FR 37188 (July 14, 2021).

Individuals have also been notified that the criminal justice information retrieved utilizing identifying particulars by Federal criminal justice entities for the purposes of providing a computerized database of NCIC files can be accessed or amended, in accordance with DOJ regulations, and in accordance with JUSTICE/FBI-001, "National Crime Information Center (NCIC)" 64 FR 52343 (Sept. 28 1999); 66 FR 8425 (Jan. 31, 2001); 72 FR 3410 (Jan. 25, 2007) (rescinded by 82 FR 24147); 82 FR 24147 (May 25, 2017); 84 FR 47533 (Sept. 10, 2019).

JWIN is not a system of record. Any FOIA requests for information stored in JWIN are handled by the authoritative record holder, such as NCIC or Nlets.

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).

	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): October 6, 2020 – Next ATO 10/06/2023 **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:** POA&M ID: POA&M Title 37408: JWIN - Strengthen session lock process.
X	42057: JWIN - Expand multi-factor authentication (MFA) to all users.
	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, JWIN has an approved ATO
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** JWIN monitors for system misuse by auditing User Agencies on an annual basis. Terminal Agency Coordinators must also report suspicion of misuse and misuse of the system to initiate investigation and evaluation of information security. Additionally, Justice Criminal Information Services (JCIS) audits its User Agencies and users a minimum of once every three years to identify risks in system use and User Agency data management to ensure Criminal Justice Information (CJI) and Federal Criminal History Record Information (CHRI) reliability, confidentiality, completeness, and accuracy as is reasonably necessary to assure fairness to the individual in any agency determination about an individual.
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:** JCIS audits its User Agencies and users a minimum of once every three years to identify risks in system use and User Agency data management to ensure CJI and CHRI reliability,

	confidentiality, completeness, and accuracy as is reasonably necessary to assure fairness to the individual in any agency determination about an individual. System logs are reviewed on a weekly basis per CJIS Security Policy section 5.4.3.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. Yes, JWIN contractors are subject to the stated above.
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:** JWIN users are required to complete CJIS Security Awareness Training (CSAT) and NCIC Training and Certification prior to obtaining access to CJI and biennially thereafter. CJIS Security Awareness Training may be accomplished in the following ways: • Using DOJ CSA provided materials via the online JCIS Training and Learning Center (CJIS Security Awareness Training slide decks); TACs must maintain an electronic log with the training information • Complete Agency INFOSEC Training with DOJ CSA CJI Handling Addendum (located on the JCIS Training and Learning Center) • Utilize an Agency-developed training program; a copy of the training and name of the training tool must be sent to DOJ.CSA.JCIS@usdoj.gov for review and approval NCIC Training and Certification may be accomplished in the following ways: • Using DOJ CSA provided materials and testing via the online JCIS Training and Learning Center (NCIC Certification Course Slides and Audio Script PDF and NCIC Certification Test) • Utilize an Agency-developed training program; a copy of the training and certification, along with the name of the training tool, must be sent to DOJ.CSA.JCIS@usdoj.gov for review and approval

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?

A full security control assessment has been completed for JWIN and all information system components. These assessments are performed to ensure compliance with Federal and DOJ requirements, and include: physical and logical access, identification and authentication, vulnerability management, auditing, and other assessment actions to ensure that security controls are operating as intended. JWIN makes use of separate Privileged and Non-Privileged user accounts and leverages

additional role-based access control technologies and administrator session recording. All system and application log data are being sent to DOJ's centralized audit log management system for triage and review. JWIN makes use of Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standard Publication (FIPS) 140-2, to protect data in transit between the browser and the user's workstation, makes use of Application Layer Firewall and integrated Intrusion Detection System / Intrusion Prevention System technology. The CSS Information Security System Officers (ISSOs) are charged with reviewing logins and performing auditing functions to ensure role-based access controls satisfy the above measures.

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.)

Pursuant to the DOJ Order 0904 Cybersecurity Program, JCIS implements the data minimization and retention requirements, which state that components will only retain PII that is relevant and necessary for the purpose for which it was originally collected. After records are no longer needed for frequent consultation, but before they are ready to be destroyed, JCIS uses the National Archive Record Administration's (NARA) General Records Schedule 3.2 Information Systems Security Records and 4.2 for Information Access and Protection Records to determine how long the records should be retained before disposition. Additionally, the CJIS Security Policy requires logs of records be retained a minimum of one year.

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:

JWIN is not a System of Record and should not require a SORN. JWIN is not the authoritative owner/source of records. JWIN transmits records from the national crime information centers NCIC, Nlets, and NGI, which serve as the source of records. JWIN passes those results to the User Agency.

Account, audit log, and user records maintained in this system for the purpose of monitoring system activity are covered by JUSTICE/DOJ-002, "Department of Justice Information Technology, Information System, and Network Activity and Access Records" 86 FR 37188 (July 14, 2021).

Criminal justice information retrieved utilizing identifying particulars by Federal criminal

justice entities for the purposes of providing a computerized database of NCIC files is covered by JUSTICE/FBI-001, "National Crime Information Center (NCIC)" 64 FR 52343 (Sept. 28 1999); 66 FR 8425 (Jan. 31, 2001); 72 FR 3410 (Jan. 25, 2007) (rescinded by 82 FR 24147); 82 FR 24147 (May 25, 2017); 84 FR 47533 (Sept. 10, 2019).

Section 8: Privacy Risks and Mitigation

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical, and physical controls over the information.***

Collecting and maintaining more personal information than necessary to accomplish the Department's official duties is always a potential threat to privacy. JWIN only collects and maintains information about an individual that is relevant and necessary to accomplish the system's purpose. JWIN collects information submitted by authorized users for the purpose of updating or locating information stored in the NCIC and Nlets, and affiliated crime information systems, such as the III and NICS. User agency submissions include Personally Identifiable Information (PII). JWIN requires authorized users to have a user account. User agencies are onboarded after signing a CJIS Systems User Agreement between the DOJ CSA and the agency. Agencies are responsible for maintaining user accounts and all agencies are audited triennially. User accounts include information about the authorized user, and may include PII, such as: user's name; telephone number, email address; and the agency/organization that employs the user.

Excluding information available to authorized system users, no information collected, handled, stored and/or accessed by this information technology within JWIN is disseminated to any other individuals or organizations.

By Department Order, all DOJ users with access to Department networks, including JWIN, must receive an annual Cyber Security Assessment Training (CSAT) which includes a Rules of Behavior (ROB) that each user must acknowledge and agree to follow. The CSAT course and ROB include information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII, identifies potential risks and vulnerabilities associated with using DOJ-owned IT systems, provides a review of the user's role in protecting these systems, and establishes guidelines to follow at work and in mobile settings to protect against attacks on IT systems. Failure to successfully complete this training and agree to the ROB can result in termination of the employee or

contractor's access to DOJ computers. Participation in the training course is tracked to ensure that DOJ employees and contractors comply with this training.

Finally, to ensure the continued relevance and effectiveness of security controls, risk assessments, and privacy and security control assessments are routinely evaluated. In accordance with the NIST Special Publication 800-53 (Rev.5), these assessments include managerial, operational, and technical controls to minimize any privacy risks.