# United States Department of Justice
# Justice Management Division

# Privacy Impact Assessment
for the
FixNICS Disposition Reporting System (FixNICS DRS)

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

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

Date approved: April 9, 2024

*(May 2022 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.)***

Pursuant to sections 501 and 524(b) of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Crime Control Act of 1973, Public Law 93-83, 87 Stat. 197, 42 U.S.C. 3701, et seq. (Act), 28 U.S.C. 534, and Public Law 92-544, 86 Stat. 1115, 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, completeness, reliability, integrity, and security of such information and to protect individual privacy.

FixNICS Disposition Reporting System (DRS) is an information system developed through a partnership project between the U.S. Federal Executive and Judicial branches. The primary project objectives for FixNICS DRS are: 1) reduce the risk of improper transfer of firearms to prohibited persons; and 2) improve the quality of criminal history information used for civil background checks, such as employment, licensing, and positions of trust. The FixNICS DRS solution achieves its objectives by matching records from and facilitating record updates of core federal criminal information systems and databases in coordination with arresting agencies. The system matches U.S. persons' federal arrest events with U.S. Courts' Judgment and Commitment (J&C) Orders and U.S. Attorneys' unique record identifiers, called National Instant Criminal Background Check System (NICS) Prohibitors[1]. Authorized users from participating federal arresting agencies (e.g., the Bureau of Alcohol, Tobacco, and Firearms (ATF), Drug Enforcement Administration (DEA), the United States Marshals Service (USMS) and Federal Bureau of Investigation (FBI)), United States Attorney's Offices (EOUSA), and U.S. Courts, will have access to the information. FixNICS was developed using a Commercial-Off-The-Shelf (COTS) product, Entellitrak[2].

Because FixNICS captures and analyzes substantial amounts of personally identifiable information (PII), a privacy impact assessment is required by Section 208 of the E-Government Act of 2002.

## Section 2: Purpose and Use of the Information Technology

***2.1 Explain in more detail than above the purpose of the 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.***

---

[1] NICS prohibitors are categories of persons, as defined under state and federal laws, prohibited from receiving firearms. For more information and a list of federally prohibiting criteria, refer to: Appeals and Voluntary Appeal File — FBI.
[2] Entellitrak - https://www.tylertech.com/products/case-management-development-platform.

The existing federal NICS system is incomplete and divided because states implement their own NICS programs and fail to submit prohibiting records. FixNICS is designed to address this issue as well as address various other challenges of the existing NICS system described below:

- Inconsistencies across multiple databases, which may lead to states allowing individuals to be granted a firearm transfer that may otherwise be prohibited.
- Arresting agencies currently submit and mail dispositions after completing the R-84 Disposition Report Form[3], creating delays and possibility for error.
- FixNICS is a consolidated system, which integrates arrest events and prohibitor data from all core criminal information systems and databases.
- The function of tracking, submitting, and reporting of prohibitor data will also be consolidated, eliminating the overhead and delayed communications between disjointed core systems
- Rather than functioning only as a database, FixNICS will also provide user interfaces allowing analysts and law enforcement agents to view and act on data.
- FixNICS provides technical capabilities such as workflow processing, exception handling, automated notifications, user-friendly dashboards, and the ability to generate relevant reports.

To accomplish these objectives, FixNICS obtains PII from the U.S. Courts Probation and Pretrial Services Automated Case Tracking System (PACTS) and court documents (e.g., Judgments, Amended Judgments) from the U.S. Courts Case Management/Electronic Case Files (CM-ECF) system. FixNICS also pulls information via the Judicial Access Browser System (JABS) from the FBI's Next Generation Identification (NGI)[4] system and from the FBI's National Crime Information Center (NCIC) via the DOJ Law Enforcement Services & Information Sharing (LESIS) Justice Web Interface to NCIC (JWIN)[5].

FixNICS combines matched J&C order details and arrest information into a single electronic data package and sends it to the relevant Federal arrest agency for validation. Upon confirmation of accuracy by the arresting agency, the system sends the validated information to JABS for submission to NGI to add/update criminal history information. Consequentially, subsequent gun transfer checks and criminal history queries executed against these core systems will generate more accurate and up-to-date information to support timely decisions. For FixNICS operations and maintenance planning and improvement activities, the system generates management reports to monitor the timely processing of NICS prohibitor records and the submission of disposition records.

---

[3] A Criminal History Record includes an individual's identifiers (e.g., descriptive information and fingerprints), arrests and subsequent dispositions. Dispositions are posted to the National Criminal History Record File by the FBI's Criminal Justice Information Services (CJIS) Division. Each criminal arrest for which the CJIS Division has a fingerprint submission should have a disposition.
The FBI defines a disposition as an action regarded by the criminal justice system to be final. A disposition states that arrest charge(s) have been modified, dropped or reports the findings of a court. Dispositions are submitted by criminal justice agencies and posted to the Criminal History Record to ensure accuracy and completeness. The R-84 is a Disposition Report Form used by criminal justice agencies to submit a Disposition Report to FBI CJIS.

[4] NGI is covered by separate privacy documentation and can be found here: https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments.

[5] JWIN is subject to separate privacy documentation and can be found here: Office of Privacy and Civil Liberties | DOJ Privacy Impact Assessments (justice.gov).

FixNICS DRS obtains data and files containing PII from the U.S. Courts PACTS and court documents (e.g., Judgments, Amended Judgments) from the U.S. Courts CM-ECF system for criminal cases adjudicated at a Federal District Court. These U.S. Court packages are transmitted through encrypted email attachments which travel over Justice Unified Telecommunications Network (JUTNet) virtual private network (VPN) tunnel.[6] The attachments are stored in the FixNICS DRS database where they are automatically matched to arrest records from JABS. FixNICS queries JABS for unique record identifiers to generate a list of corresponding/matching records. If no matching record is found, FixNICS Analysts research and modify the query within FixNICS DRS to find candidate matches. For example, analysts may remove specific unique record identifiers to expand search results that generate a broader set of candidate record matches. FixNICS also operates within its own technical and security boundary, separate and apart from JABS. FixNICS interacts with JABS through established DOJ and FBI communications channels.

When a matching arrest record is found, FixNICS creates a Disposition Report using court charges and sentence information from the U.S. Courts information and the offender's PII, date of arrest, and arrest information from the JABS arrest record. Arresting agencies are notified by FixNICS to confirm or reject the matching arrest records and Disposition Report within FixNICS DRS.

Before submitting the Disposition Report, within FixNICS the arresting agency reviewers can search for an offender's criminal history record in NCIC to view the arrest record to see if it has a disposition posted earlier (e.g., a disposition posted based on a past court judgment). The analyst can then take proper action (e.g., add, append, replace, delete) in reporting the current court disposition (e.g., append new sentence information from the amended judgment) to avoid accidentally overwriting or deleting important information. FixNICS DRS has an interface with the JWIN system to search for criminal history records in NCIC.

A confirmed Disposition Report is returned to FixNICS and submitted via JABS to the NGI system. The NGI system processes the disposition to update the offender's criminal history record and keep it current. NGI does not return a copy of the offender's updated criminal history record showing the disposition was updated. Within FixNICS, the arresting agency reviewer can do another search in NCIC to be confident that the criminal history record was updated in a manner consistent with the reviewer's intent when submitting the Disposition Report.

As a Criminal Justice Information Services Division (CJIS) System Agency (CSA)[7], the LESIS program office tracks disposition reporting activity for arrests submitted via JABS to NGI. Some arresting agencies are currently using other methods to submit dispositions electronically to FBI CJIS. USMS submits disposition reports via JABS to NGI. DEA submits disposition reports via JWIN to NCIC. FixNICS obtains a copy of USMS dispositions files from JABS and a copy of DEA dispositions via a report produced by JWIN staff. FixNICS correlates the USMS and DEA dispositions to their respective corresponding arrest records in JABS so that FixNICS can produce metrics on the percentage of arrests that have dispositions submitted electronically to FBI CJIS.

---

[6] A virtual private network (VPN) is a virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. *See* virtual private network (VPN) - Glossary | CSRC (nist.gov).

[7] A CSA is a criminal justice agency that oversees administration and usage of the CJIS Division programs within a state, district, territory, or country.

As noted earlier in this document, FixNICS is a consolidated system that integrates arrest data, court records with dispositions to update criminal history records, and EOUSA's NICS Prohibitor records. EOUSA has been submitting NICS Prohibitors via the JWIN interface to NCIC/NICS Indices for 10+ years. The EOUSA CaseView system creates the NICS Prohibitors and provides the files to the JABS staff. JABS staff re-formats the data into the NCIC format and submits the NICS Prohibitors via JWIN to NCIC/NICS Indices. FixNICS obtains a copy of the EOUSA NICS Prohibitors from JABS and correlates the Prohibitor records to the corresponding cases adjudicated at U.S. Federal District Courts for the purpose of assessing the timeliness and completeness of EOUSA NICS Prohibitor submissions to NCIC/NICS Indices.

***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 | Consolidated Appropriations Act ("Fix NICS Act") of 2018 (Pub. L. 115-141, March 23, 2018, codified in relevant part at 34 U.S.C. § 40901); 28 U.S.C. § 534; see also 8 U.S.C. §§ 1324, 1357(f)-(g); 28 U.S.C. §§ 564, 566; 5 U.S.C. § 301; 44 U.S.C. § 3101; 31 U.S.C. Part 501; 18 U.S.C. §§ 3621, 4003, 4042, 4082, 4086; 26 U.S.C. § 7608; Comprehensive Drug Abuse Prevention and Control; Act of 1970 (Pub. L. No. 91-513), 21 U.S.C. § 801 et seq.; Reorganization Plan No. 2 of 1973 (Pub. L. No. 93-253) |
| Executive Order | |
| Federal regulation | 28, Code of Federal Regulations, Part 20, Criminal Justice Information Systems |
| Agreement, memorandum of understanding, or other documented arrangement | Memorandum of Understanding (MOU)<br>Between The Administrative Office of the U.S. Courts and The U.S. Department of Justice (DOJ) On Data Sharing, October 2012;<br><br>User Agency Agreement Between<br>U.S. Department of Justice Criminal Justice Information Services Systems Agency and<br>Bureau of Alcohol, Tobacco, Firearms, and Explosives, 8/6/20 |
| Other (summarize and provide copy of relevant portion) | |

## Section 3: Information in the Information Technology

***3.1 Indicate below what types of information that may be personally identifiable in Column (1)***

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

| (1) General Categories of Information that May Be Personally Identifiable | (2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row) | (3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public Non USPERs | (4) Comments |
|---|---|---|---|
| *Example: Personal email address* | *X* | *B, C and D* | *Email addresses of members of the public (US and non-USPERs)* |
| **Name** | X | C and D | Legal names and known aliases as collected by law enforcement and U.S. Courts. |
| **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** | | | |
| **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)** | | | |
| **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** | | | |
| **Mother's maiden name** | | | |
| **Vehicle identifiers** | | | |
| **Personal mailing address** | X | C and D | Personal mailing address 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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public Non USPERs | (4) Comments |
|---|---|---|---|
| **Personal e-mail address** | | | |
| **Personal phone number** | | | |
| **Medical records number** | | | |
| **Medical notes or other medical or health information** | | | |
| **Financial account information** | | | |
| **Applicant information** | | | |
| **Education records** | | | |
| **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** | | | |
| **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** | | | |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public Non USPERs | (4) Comments |
|---|---|---|---|
| **Grand jury information** | X | C and D | Grand Jury information for members of the public (both USPERs and non-USPERs) |
| **Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information** | | | |
| **Procurement/contracting records** | | | |
| **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 and B | Date/time of access of DOJ/Component Employees, Contractors, Detailees and other Federal Government Personnel |

| (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:<br>A. DOJ/Component Employees, Contractors, and Detailees;<br>B. Other Federal Government Personnel;<br>C. Members of the Public US Citizens or Lawful Permanent Residents (USPERs);<br>D. Members of the Public Non USPERs | (4) Comments |
|---|---|---|---|
| - **User passwords/codes** | X | A and B | Queries run of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel |
| - **IP address** | X | A and B | Content of files accessed/reviewed of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel, which may show IP addresses. |
| - **Date/time of access** | X | A and B | Date/time of access of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel |
| - **Queries run** | X | A and B | Queries run of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel |
| - **Contents of files** | X | A and B | Contents of files accessed/reviewed of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel |
| **Other (please list the type of info and describe as completely as possible):** | X | A and B | The contents of files of DOJ/Component Employees, Contractors, Detailees, and other Federal Government Personnel and information contained in criminal history data of members of the public may contain additional types of PII. |

### *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 | Other federal entities | X |

| **Government sources:** | | | | | |
|---|---|---|---|---|---|
| State, local, tribal | X | Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer) | | | |
| Other (specify): The primary source of information is data collected by U.S. Courts and DOJ Components. This information collected may include information that was initially collected from other entities, such as NCIC. | | | | | |

| **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 | Authorized JMD personnel can login to FixNICS DRS 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 FixNICS DRS (or leverage a system interconnection) to query or update records stored in national crime information systems, such as NCIC. |

| 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.** |
| Federal entities | | | X | Authorized users within Federal entities can login to FixNICS DRS to query or update records stored in national crime information systems, such as NCIC. |
| State, local, tribal gov't entities | | | X | Law enforcement agencies will log in through a web interface (Law Enforcement Enterprise Portal)[8] |
| Public | | | | |
| Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes | | | | |
| Private sector | | | | |
| Foreign governments | | | | |
| Foreign entities | | | | |
| Other (specify): | | | | |

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

Information from FixNICS 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.***

FixNICS does not collect information directly from individuals, rather information is collected from source systems PACTS, CM-ECF, NGI and NCIC. Due to the law enforcement nature of these systems, individual notice is generally not provided. Agencies contributing information to FixNICS

[8] The Law Enforcement Enterprise Portal (LEEP) is covered under separate privacy documentation, available here: https://www.fbi.gov/file-repository/pia-leep-070319.pdf/view.

likely do not provide any individual Privacy Act Statement or other notice to the individuals about whom the information pertains. Non-federal contributors are not subject to the Privacy Act; federal contributors are exempted from the Privacy Act's individual notice provisions in connection with criminal law enforcement activities.

However, multiple SORNs provide generalized notice to individuals, including JUSTICE/DOJ-005, "Nationwide Joint Automated Booking System (JABS);" 71 FR 52821 (Sept. 7, 2006), JUSTICE/FBI-018, "National Instant Criminal Background Check System (NICS)," 84 FR 54175 (Oct. 31, 2019), 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), and JUSTICE/FBI-009, "The Next Generation Identification (NGI) System;" 84 FR 54182 (Oct. 9, 2019).

***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.***

FixNICS DRS does not collect information directly from individuals 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 FixNICS DRS are handled by said systems, such as U.S. Courts, NGI, and NCIC. However, given the law enforcement nature of the information, these systems are likely exempt from certain provisions of the Privacy Act.

***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.***

Any Freedom of Information Act or Privacy Act requests for information stored in FixNICS DRS are handled by the authoritative record holder, such as U.S. Courts, NGI, and NCIC. Individuals may also follow the procedures outlined in Subpart D, Part 16, Title 28, Code of Federal Regulations. The records maintained in FixNICS DRS, however, may be subject to certain exemptions to the access and amendment procedures, as articulated in the applicable SORNs, above, and in Subpart E, Part 16, Title 28, Code of Federal Regulations.

## 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):** |

| | |
|---|---|
| | Issued: 8/25/23 Expires: 8/24/2024<br>**If an ATO has not been completed, but is underway, provide status or expected completion date:**<br>**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:**<br>The system has been categorized as High for Confidentiality, Availability, and Integrity. |
| X | **Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:**<br>FixNICS DRS continuously monitors for system misuse. Functionality is developed and tested in the DOJ Test environment. Terminal Agency Coordinators (TACs) must also report suspicion of misuse of the system to the FixNICS DRS Incident Response Team which initiates investigation and evaluation of potential security violations and impacts. Additionally, Splunk audit logs are generated for the ISSO to monitor valid and invalid user access attempts. Splunk dashboards are generated weekly for review and contain key system events, alerts, and metrics to support quick identification of anomalous activity within FixNICS DRS. |
| 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:**<br>Audit procedures consist of patch update and vulnerability scans to determine if security standards are being met. Tenable Nessus and BigFix scans are performed to determine if any known vulnerabilities exist in operating systems, software applications, and configuration components of the system. These scans determine if known vulnerabilities are present in the system, duration of exposure, and severity level. System logs are reviewed on a weekly basis by the ISSO 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**.<br>All contractors are required to take annual DOJ information security privacy and awareness training. |
| 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:**<br><br>FixNICS DRS users are required to complete CJIS Security Awareness Training and NCIC Training and Certification prior to obtaining access to CJIS and biennially thereafter.<br><br>CJIS Security Awareness Training may be accomplished in the following ways:<br>• Using DOJ CSA provided materials via the online Justice Criminal Information Services (JCIS) Training and Learning Center (CJIS Security Awareness Training slide decks); TACs must maintain an electronic log with the training information<br>• Complete Agency INFOSEC Training with DOJ CSA CJI Handling Addendum (located on the JCIS Training and Learning Center)<br>• 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<br>• Privileged users such as Administrators received specialized training.<br><br>NCIC Training and Certification may be accomplished in the following ways:<br>• 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)<br>• 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?***

FixNICS DRS employs separate Privileged and Non-Privileged user accounts, leverages additional role-based access control technologies, and records administrator sessions. FixNICS DRS also implements Application Layer Firewall[9] and integrated Intrusion Detection System / Intrusion Prevention System[10] technology to protect and monitor data in transit over its network infrastructure.

[9] A firewall is a device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. By employing firewalls to control connectivity to these areas, an organization can prevent unauthorized access to its systems and resources. *See* https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf.

[10] IDS/IPS is a security service that monitors and analyzes network or system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner. See https://csrc.nist.gov/glossary/term/intrusion_detection_system.

All system and application log data are sent to DOJ's centralized audit log management system for triage and review. Information Security System Officers (ISSOs) review logins and perform audit functions to ensure account policies, safeguards, and access controls meet the established policy and security requirements.

Inbound data from external agencies (U.S. Courts) is encrypted through secure e-mail and hypertext transfer protocol secure (https) over transport layer security (TLS) 1.2[11]. Social Security numbers (SSNs) are encrypted as a part of the email packages sent to FixNICS DRS over an encrypted VPN tunnel. Additionally, the databases storing the records (which include PII such as SSNs) within DOJ are encrypted. FixNICS uses MS SQLServer's Transparent Data Encryption (TDE) to encrypt data at rest.[12] These records are viewable in plain text to FixNICS DRS analysts while using the system as this is a data point to validate matching J&C packages to JABS records. The matches are reviewed and submitted by the arresting agency and while the FixNICS analysts perform manual matching, they do not submit dispositions. As a mitigating control, FixNICS uses Secure Sockets Layer (SSL) encryption, compliant with the Federal Information Processing Standards Publication (FIPS) 140-2[13], to protect data in transit between the FixNICS DRS Application Server and the user's workstation. Encryption redundancy also exists for backup data (i.e. backup data is also encrypted at rest).

An initial security control assessment has been completed for FixNICS DRS and all information system components. These assessments are performed to ensure compliance with Federal and DOJ security and privacy 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.

***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 states 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 Archives and Records 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***

---

[11] https and TLS are encryption protocols that allow for the secure transmission of information.
[12] Data at rest encryption ensures that data is stored in an encrypted format.
[13] FIPS 140-2 can be found here: https://csrc.nist.gov/pubs/fips/140-2/upd2/final.

***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:***

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).

JUSTICE/FBI-018, "National Instant Criminal Background Check System (NICS)," 84 FR 54175 (Oct. 31, 2019).

JUSTICE/DOJ-005, "Nationwide Joint Automated Booking System (JABS);" 71 FR 52821 (Sept. 7, 2006).

JUSTICE/FBI-009, "The Next Generation Identification (NGI) System;" 84 FR 54182 (Oct. 9, 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. FixNICS DRS only collects and maintains information about an individual that is relevant and necessary to accomplish the system's purpose. FixNICS DRS collects information submitted by authorized users for the purpose of updating or locating information stored in the NCIC and JWIN to access criminal history records in National Instant Criminal Background Check System (NICS). Any user agency submission may include PII. FixNICS DRS requires authorized users to have a user account. 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. Information is encrypted at rest and in transit using the protocols outlined in Section 6.2. In addition, when information is being input into the system, the information is validated by human reviewers multiple times, e.g., personnel at the arresting agency, as explained in the response to question 2.1 above.

Only authorized system users may access the system to access the information contained in it. Other than authorized system users, and authorized auditors or other oversight bodies or through legal proceedings, no information collected, handled, stored and/or accessed by this information technology within FixNICS DRS is disseminated to any other individuals or organizations.

By Department Order, all DOJ users with access to Department networks, including FixNICS DRS, must receive an annual Cyber Security Awareness Training (CSAT). The CSAT course includes information on certain federal information privacy laws, such as the Privacy Act, and requirements for proper handling of PII. The course 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. All employees and contractors must also annually sign a DOJ Rules of Behavior agreement confirming that they have completed this course and that they agree to abide by such requirements reviewed in the course. Failure to successfully complete this training 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. Specialized training is provided for FixNICS DRS System Administrators with privileged access as well.

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 risk.