Federal Bureau of Investigation

Privacy Impact Assessment
for the
[National Data Exchange (N-DEx) System]

Issued by:
Erin M. Prest, Privacy and Civil Liberties Officer

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

Date approved: September 9, 2022

(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 National Data Exchange (N-DEx) System is a national online investigative information sharing system that brings together criminal justice records from across the nation. Federal, state, local, tribal and territorial criminal justice data, including federated foreign and international data, is available 24 hours a day, 7 days a week from any secure internet capable device. Investigators and analysts have the ability to discover information from across the nation in one system which will display the entire criminal justice life cycle, from initial contact with a suspect, to the subject's release from prison, as well as probation and parole information regarding criminal justice subjects. More information about the N-DEx System is available online at https://www.fbi.gov/services/cjis/ndex.

This Privacy Impact Assessment (PIA) provides an overview of the N-DEx System and assesses the risks associated with the maintenance, retrieval, and use of the information for criminal justice purposes; criminal justice employment background checks; fitness determinations made by federal executive agencies pursuant to Executive Order 13467, as amended by Executive Order 13746; background checks for firearms, explosives, and associated licenses/permits; and security risk assessments completed on individuals applying for access to select biological agents or toxins. This PIA supersedes the previously published PIAs https://www.fbi.gov/file-repository/pia-national-data-exchange-n-dex-system.pdf/view, updates terminology, discusses data integration and data analysis services, and covers all current information within, and functionality of, the N-DEx System.

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 N-DEx System provides a national investigative information sharing system available through a secure Internet site that allows criminal justice agencies (CJAs),[1] and limited authorized

[1] CJAs are the courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. See 28 C.F.R. § 20.3(g). Examples include criminal justice law enforcement agencies (see next footnote), prosecuting attorney's offices, pretrial service/pretrial release agencies, correctional institutions, probation and parole offices, courts and magistrates offices, custodial facilities in medical or psychiatric institutions and some medical examiners' offices which are criminal justice in function, regional dispatch centers which are criminal justice agencies or noncriminal justice governmental agencies performing criminal justice dispatching functions for criminal justice agencies, state and federal inspectors general offices, and local, county, state, or federal agencies that are classified as criminal justice agencies by statute but do not fall into one of the aforementioned categories. CJAs also include nongovernmental railroad or campus police departments qualifying for access to criminal history record information.

noncriminal justice agencies, to search and analyze data representing the entire criminal justice cycle, including crime incident and investigation records; arrest, booking, and incarceration records; and probation and parole records. Managed by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division, the N-DEx System is a major component of the Department of Justice (DOJ) Law Enforcement Information Sharing Program's (LEISP) strategy. A principal purpose of the LEISP is to ensure DOJ criminal law enforcement information is available to users at all levels of government so they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect national security.

As a repository of information from federal, state, local, tribal, territorial, and foreign criminal justice entities, the N-DEx System provides these agencies with the capability to link crime incidents, criminal investigations, and related events to help solve, deter, and prevent crimes, and thereby improve national security. At its initial deployment, access to the N-DEx System was only available to certain federal CJAs and select local and state criminal justice law enforcement agencies[2] in the United States. The N-DEx System was primarily used to share and manage incident and case reports, arrest data, and both open and closed investigative cases among those users, using data sharing policies and role-based access controls. Since then, the N-DEx System has become a valuable information sharing tool that is available to all U.S. CJAs and limited authorized noncriminal justice agencies. The use of the N-DEx System has expanded to include access to its data for firearm, explosive, and associated license/permit related background checks; security risk assessments for individuals applying for access to select biological agents and toxins under 42 U.S.C. § 262a;[3] and fitness/suitability determinations conducted by federal executive agencies in accordance with Executive Order 13467, as amended by Executive Order 13764.

As listed in Section 2.2, the FBI has statutory authority to collect, preserve, and exchange criminal justice and law enforcement related information. The N-DEx System was created consistent with the authority to establish a secure national criminal justice information sharing capability. The N-DEx System contains and disseminates information collected and contributed by criminal justice agencies pursuant to and compliant with all applicable federal, state, local, tribal, and territorial laws, and agency regulations, policies, and procedures. The N-DEx System provides the ability for criminal justice agencies, and limited authorized noncriminal justice agencies, to search and analyze information relevant to their missions. The N-DEx System enables users to discover information and make associations which promote the enforcement of criminal law and the administration of criminal justice. Expanded use of the N-DEx System for firearm-related checks and security risk assessments provides access to additional criminal justice information relevant in determining if a potential firearm or explosive transferee is prohibited by federal or state law from receiving a firearm, explosive, or associated permit, or if an applicant is legally restricted from having access to select biological agents or toxins.

In addition to maintaining an operational environment for criminal justice agencies to share information, the N-DEx Program Office includes system data integration (DI) and data analysis/data quality (DA/DQ) services. The DI and DA/DQ teams are part of the N-DEx Program Office. All DI

---

[2] Criminal justice law enforcement agencies are a subcategory of CJAs consisting of governmental agencies or subunits thereof having statutory power of arrest and whose primary function is that of apprehension and detection. Examples include police, sheriff, FBI, the Drug Enforcement Administration (DEA), and criminal justice task forces.

[3] The Bioterrorism Risk Assessment Group conducts risk assessments under 42 U.S.C. § 262a; https://www.fbi.gov/file-repository/pia-brag-database.pdf/view.

and DA/DQ activities occur in a nonoperational environment. The DI team conducts development activities on copies of data from CJAs and assists agencies in mapping their data to the N-DEx submission standard. The N-DEx Program Office provides this service because many agencies do not have the funding, knowledgeable staff, or the time to map the data to the N-DEx standard. The agencies' data is used in the mapping process to create a better adapter, requiring less agency support during the writing and quality assurance (QA) process. The DA/DQ team analyzes copies of the agencies' data to obtain the best quality criminal justice data for ingestion into the N-DEx System. The DA/DQ system provides continual data quality feedback to internal and external stakeholders regarding the quality of the data, so improvements can be made for future record submission.

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

	Authority	Citation/Reference
X	Statute	28 U.S.C. 533, 534; 34 U.S.C. 10211; 44 U.S.C. 3301
	Executive Order	
X	Federal Regulation	28 C.F.R. 0.85; 28 C.F.R. Part 20
X	Agreement, Memorandum of Understanding, or other documented arrangement	CJIS User Agreement
X	Other (summarize and provide copy of relevant portion)	*CJIS Security Policy; N-DEx System Policy and Operating Manual*

Section 3: Information in the Information Technology

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

The N-DEx System contains the personally identifiable information (PII) of suspects, perpetrators, witnesses, victims, and anyone else who may be identified in criminal justice information. This includes anyone named in pre-trial investigations; arrest, booking, and incident reports; incarceration reports; and probation and parole reports. The system also includes contact information of individuals and agencies contributing data to the N-DEx System and designated as N-DEx System record points of contact. PII contained within the N-DEx System may include, but is not limited to: name; sex; race; citizenship; date and place of birth; address(es); telephone number(s); email address(es) and internet identifiers; social security number(s) or other unique identifiers; physical description (including height, weight, hair color, eye color, gender); occupation and vehicle identifiers; and photographs. The incident, offense, and other criminal justice reports are comprised of structured information fields that allow the N-DEx System to automatically correlate the names, addresses, telephone numbers, offense locations, type of weapon, and other data elements in the

reports against one another to identify potential links. All reports are submitted to the N-DEx System by each criminal justice agency pursuant to, and compliant with, the agency's own state laws, guidelines, regulations and agency policies and practices. The chart below sets forth the type of information that may be contained in the N-DEx System.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	Due to the large number and variety of criminal justice records contained in the N-DEx System, it is likely that many different personal identifiers, including identifying numbers and general personal data, will be contained in the records.
Date of birth or age	X	A, B, C, D	See above.
Place of birth	X	A, B, C, D	See above.
Gender	X	A, B, C, D	See above.
Race, ethnicity or citizenship	X	A, B, C, D	See above.
Religion	X	A, B, C, D	See above.
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, D	Social security numbers often appear in criminal justice records to distinguish one individual from another.

(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
Tax Identification Number (TIN)	X	A, B, C, D	Due to the large number and variety of criminal justice records contained in the N-DEx System, it is likely that many different personal identifiers, including identifying numbers and general personal data, will be contained in the records.
Driver's license	X	A, B, C, D	See above.
Alien registration number	X	A, B, C, D	See above.
Passport number	X	A, B, C, D	See above.
Mother's maiden name	X	A, B, C, D	See above.
Vehicle identifiers	X	A, B, C, D	See above.
Personal mailing address	X	A, B, C, D	See above.
Personal e-mail address	X	A, B, C, D	See above.
Personal phone number	X	A, B, C, D	See above.
Medical records number	X	A, B, C, D	Medical records numbers may be present if they are part of a criminal justice report.
Medical notes or other medical or health information	X	A, B, C, D	Medical notes and medical/health information may be present if part of a criminal justice report.
Financial account information	X	A, B, C, D	See above.

(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
Applicant information	X	A, B, C, D	Unless part of a criminal justice report, applicant information would only be maintained in the N-DEx System search history for searches conducted for criminal justice employment background checks or federal suitability determinations.
Education records	X	A, B, C, D	Education records may be present if they are part of a criminal justice report.
Military status or other information	X	A, B, C, D	See above.
Employment status, history, or similar information	X	A, B, C, D	See above. In addition, the N-DEx System maintains limited employment information on its users to ensure they qualify for access to the system (e.g., employing agency).
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates	X	A, B, C, D	The N-DEx System maintains N-DEx training completion certificates for its 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
Legal documents	X	A, B, C, D	Due to the large number and variety of criminal justice records contained in the N-DEx System, it is likely that many different types of general personal data will be contained in the records.
Device identifiers, e.g., mobile devices	X	A, B, C, D	See above. If a user accesses the N-DEx System with a mobile device, the N-DEx System will display the N-DEx mobile view to the user.
Web uniform resource locator(s)			
Foreign activities	X	A, B, C, D	Foreign activity information may be present if part of a criminal justice report. In addition, the N-DEx System can capture an Interpol-assigned identification number. The N-DEx System also federates a search of Interpol records, but the records are not maintained within the N-DEx system.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	Due to the large number and variety of criminal justice records contained in the N-DEx System, it is likely that many different types of general personal data will be contained in the records.
Juvenile criminal records information	X	A, B, C, D	See above.
Civil law enforcement information, e.g., allegations of civil law violations	X	A, B, C, D	See above.
Whistleblower, e.g., tip, complaint or referral	X	A, B, C, D	The N-DEx System does not target collection of whistleblower information; however, whistleblower information may be present if part of a criminal justice report.
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, D	Due to the large number and variety of criminal justice records contained in the N-DEx System, it is likely that many different types of personal data, including personal data about witnesses, will be contained in the records.
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	X	A, B, C, D	This information may be present if part of a criminal justice report.
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	See above. The N-DEx System does not employ location tracking capabilities.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C, D	These biometric images can be retrieved if associated with a relevant biographic record; however, the N-DEx System is not a biometric system and biometrics contained therein are not independently searchable. Information returned to users from a federated search of a system could include biometric information, such as fingerprints, palm prints, and DNA and dental profiles.
- **Video containing biometric data**			
- **Fingerprints**	X	A, B, C, D	See above.
- **Palm prints**	X	A, B, C, D	See above.
- **Iris image**			
- **Dental profile**	X	A, B, C, D	See above.
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, D	See above.
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**	X	A, B, C, D	See above.

(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 (specify)**			
System admin/audit data:			
- **User ID**	X	A, B, C, D	Audit logs also capture the agency ORI. For noncriminal justice queries, only the following information is included in the audit log: N-DEx System user's First and Last Name, Agency ORI, Use Code, and Search Reason (when utilizing the web service).
- **User passwords/codes**			
- **IP address**	X	A, B, C, D	See above.
- **Date/time of access**	X	A., B, C, D	See above.
- **Queries run**	X	A, B, C, D	See above.
- **Content of files accessed/reviewed**	X	A, B, C, D	See above.
- **Contents of files**	X	A, B, C, D	See above.
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Explanatory data providing details about the reported events (e.g., crime incidents, investigations, arrests, bookings, incarcerations, probation, parole, etc.) and associated reports, procedures, and actions taken in the administration of criminal justice, as described in Section 1.

In addition to information contained within the N-DEx System, the N-DEx System disseminates information on individuals from other databases which can be searched via the N-DEx

System as discussed in Section 4.1. Information retrieved through a federated search of another database may include criminal justice information as described above, but may also include information on individuals identified in criminal intelligence information.

It is important to note that all the information contained within or disseminated by the N-DEx System is already collected by criminal justice agencies when fulfilling their official criminal justice functions. The N-DEx System aggregates already existing criminal justice information and then searches the data for linkages. The N-DEx System makes linkages between the criminal justice information that were previously not apparent. The N-DEx System Entity Resolution automatically resolves records into entities by partitioning data, matching and grouping records, and building one entity view of the correlated data, known as a resolved entity. It identifies relationships among persons and records and discovers hidden connections, such as common names or shared locations. It adds more meaning and context to data by allowing a user to quickly view all the data available about the subject of interest, organized for comprehension. The N-DEx System builds a virtual 'baseball card' of everything known about a subject across all incoming data streams, exposing disparate groupings of subject data to powerful search capabilities. Analysts get back information about the subject they are interested in without having to manually review and correlate hundreds of false positives. With the help of the N-DEx System Entity Resolution, users can spend time investigating and analyzing data, not finding and organizing it.

In addition, audit logs will indicate to system users if other users have accessed the same data, thereby making connections among queries more transparent. Audit logs also capture the search criteria for all criminal justice searches conducted in the N-DEx System; consequently, audit logs contain PII on any individuals searched through the N-DEx System for criminal justice purposes. Search criteria for all noncriminal justice searches conducted in the N-DEx System (i.e., Use Codes B, F, and S) is not recorded in the audit logs; PII for individuals searched through the N-DEx System solely for federal suitability checks, firearm background checks, and security risks assessments is not captured in the audit logs.

The N-DEx System provides computer-based training (CBT) modules that are the foundation of N-DEx System training. The CBT modules allow users to go through examples, practice system functions, and perform exercises. (CJA representatives can also receive the CBT modules on compact disks). Two N-DEx System CBT modules are currently available (requiring approximately 30 minutes per module to complete) and are designed to be taken by users of the N-DEx System. Additional resources available to N-DEx System users include, but are not limited to, video tutorials, Distance Learning Workshops, and quick reference cards. Information used for training resources contains no real N-DEx System records. Only test record information is used.

For N-DEx users that access the N-DEx System via the Law Enforcement Enterprise Portal (LEEP),[4] the N-DEx System provides access to a collaboration website known as JusticeConnect. JusticeConnect is a criminal justice network, available only on LEEP, which facilitates information sharing, partnership development, and project management for federal, state, local, tribal, and

[4] LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems (such as the N-DEx System) and ensuring that only authenticated users have access to those systems and services. LEEP has separate privacy documentation.

territorial partners in a secure environment. This website allows N-DEx System users to collaborate with other users by forming groups to share information, establishing discussion forums, and administering and managing group members and permissions. The collaborative environment allows the N-DEx System users to instantly and securely share pertinent information, including images, videos, charts, graphs, notes, and case reports, via any type or size of file. JusticeConnect has separate privacy documentation.

For system access control and audit purposes, the N-DEx System also contains biographic and contact data, access-authorization information, and system usage records about employees of the criminal justice agencies and limited authorized noncriminal justice agencies who have access to the N-DEx System.

The DI team operates on copies of databases obtained from agencies who desire to submit data to the N-DEx System. These databases are housed for the sole purpose of creating the applications or "adapters" which will reside on the agency's system, poll their database, and submit records to the N-DEx System. These databases contain the same type of information discussed above. In many instances, these databases are stored for retrieval at a later time to improve or upgrade the adapters. Stored databases are encrypted and only available to N-DEx Program Office and Information Technology Management Section (ITMS) N-DEx staff.

The DA/DQ team operates on copies of N-DEx System data obtained from the N-DEx operational environment. This data is transformed and stored in a data warehouse, where it can be queried, further transformed, and used for analysis and reporting purposes. From this data, the DA/DQ team provides reports and metrics for internal N-DEx Program Office use. The DA/DQ team also creates reports, at the request of a submitting agency, involving the quality of the agency's data being sent to the N-DEx System. N-DEx System information exported for DA/DQ purposes is encrypted and only available to the N-DEx Program Office and ITMS/N-DEx staff.

Lastly, the N-DEx System maintains test records for Logical Entity eXchange Services (LEXS) Search and Retrieve (SR) web service connecting agencies to use in testing their implementation of the N-DEx 4.0 Information Exchange Package Documentation (IEPD) specification. The records consist of fictional structured and unstructured data. The N-DEx System provides test records in the operational environment to allow these agencies to test their data configurations to ensure they meet N-DEx 4.0 IEPD standards. To check the accuracy of their system configurations, agencies can enter predefined search criteria which should return the test records. Test records in the operational environment are excluded from entity correlation (i.e., they are formatted so they do not correlate with other records).

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): The criminal justice records contained in the N-DEx System are submitted by federal, state, local, tribal, and territorial (to include the FBI) criminal justice agencies that collect the information. Many of these agencies collect the information directly from the individual (e.g., the suspect or complainant) during the course of their investigations.					

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)			
Other (specify): The N-DEx System does not obtain information directly from any foreign government sources; however, foreign information may be disseminated from the N-DEx System if it is submitted by a federal, state, local, tribal, and territorial criminal justice agency, or if it is retrieved via a federated search to the United States National Central Bureau's (USNCB's) International Criminal Police Organization (INTERPOL) database.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): Nongovernmental railroad or campus police departments which qualify for access to criminal history record information.					

Information is transmitted to and from the N-DEx System via multiple means. The N-DEx Program Office provides four options for agencies to submit data to the N-DEx System: secure file transfer protocol (SFTP), web services, physical media, and the N-DEx System manual web portal.

1. SFTP

SFTP servers are used for secure data submission over the Internet. Agencies submit files to a directory on N-DEx/Enterprise File Transfer Service (EFTS). Accounts are established for agencies by exchanging security keys. Agencies can submit data manually or with a data adapter, which is the most common method. The preferred method of connectivity is via the Internet; however, CJIS Wide Area Network (WAN) and Virtual Private Network (VPN) connections are also supported. Agencies have complete control over the submission process by manually connecting to the agency's SFTP directory and copying the files into the directory. This submission method increases efficiency by eliminating the possibility of human error. All data transmitted via SFTP is encrypted using Federal Information Processing Standards (FIPS) 140-2[5] approved encryption methods.

2. Web Service

Web services provide the ability for one agency's system to communicate securely to another

[5] FIPS 140-2 is available at: https://csrc.nist.gov/publications/detail/fips/140/2/final.

agency's system over the Internet. Web services are designed to allow agencies to communicate even if the agencies are using different technologies. The N-DEx System offers a data submission web service using Logical Entity eXchange Specification (LEXS) Publish and Discovery (PD). LEXS PD allows submitting agencies' systems to send single documents to the N-DEx System on a more frequent basis. Customers are required to create a web services client conforming to the N-DEx System standards and invoke the N-DEx System Ingest Web Service. The preferred method of connectivity is via the Internet; however, CJIS WAN and VPN connections are supported.

3. Physical Media

For agencies with no means to electronically transmit data to the N-DEx System, an external physical media device (CD, DVD, hard drive, etc.) may be used. Due to the sensitivity of the data and potential for PII, all data on the physical media must be encrypted before submission to the CJIS Division. The physical media must be sent to the CJIS Division using a secure traceable method, such as FedEx or United Parcel Service.

4. N-DEx System Web Portal

Agencies with a low number of incident reports or no electronic record management system may log into the N-DEx System web portal and manually type incident information into an online form. This method does not require an agency to map their data to one of the N-DEx System specifications.

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	Users have general direct access, but access to specific records depends on the user category. General access may be limited to certain information types or sources. Moreover, each record submitter can further restrict access to the record on a case-by-case basis. See narrative below for more information.
DOJ Components			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				

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.**
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			On a case-by-case basis, authorized N-DEx System users may use information retrieved from the N-DEx System for litigation purposes if the record owning agency has authorized its use.
Private sector				
Foreign governments				
Foreign entities				
Other (specify): Non-government railroad/campus police deemed appropriate for sharing.			X	Users have general direct access, but access to specific records depends on the user category. General access may be limited to certain information types or sources. Moreover, each record submitter can further restrict access to the record on a case-by-case basis. See narrative below for more information.

Access to information in the N-DEx System is restricted to criminal justice agencies and limited authorized noncriminal justice agencies. Not all users have access to all data in the N-DEx System; instead, access is determined by agency established data sharing rules and need to know. Much of the information in the N-DEx System is sensitive, and in the case of victim and witness information it is highly sensitive and potentially subject to separate protections by law. In recognition of the sensitivity of the information, the N-DEx System permits each contributing agency to control the records it submits to the N-DEx System to ensure only necessary and appropriate information is entered into the system and accessed by users with a need to know. Legal or policy restrictions can be incorporated into the sharing rules for N-DEx System information through a configurable set of tools that allow contributing agencies the flexibility to control with whom and how their information is shared and disseminated. This strategy allows agencies to submit information to the N-DEx System and share information for correlation purposes, while still controlling its dissemination.

Information may be shared under three different rule sets, designated as Green, Yellow, and Red.

Green Level Data: If the submitter of a data record has designated it to be fully shared, then all N-DEx System users with the appropriate access authority will have access to the full record and all data elements within the record.

Yellow Level Data: If the data submitter decides access to a specific record or specific data elements should be restricted except under certain circumstances, the data submitter can designate the record accordingly using pointer-based sharing. With pointer-based sharing, any user who gets a "hit" or attempts access to a record with this designation will be provided with information only on how to contact the designated record submitter. It is then the responsibility of the data requestor to contact the data submitter who will determine whether the record can be shared. If so, the N-DEx System provides mechanisms allowing the data submitter to make the record accessible to a specific user or group of users.

Red Level Data: There are circumstances where data in a record is so highly sensitive that the data contributor completely restricts access to it and to any knowledge of the record from a user group. By including the record in the N-DEx System but restricting knowledge of the record from selected users, the data submitter still benefits from correlations made with other N-DEx System records without compromising the information contained in the sensitive record.

In addition to data sharing levels set by contributing agencies, access to data within the N-DEx System is also controlled by use code. The N-DEx System currently has six use codes that correspond with authorized purposes for accessing N-DEx System data:

Criminal Justice, Use Code "C": As the foundation for the creation of the N-DEx System, use code "C" is used to share criminal justice information with criminal justice agencies for criminal justice purposes. Criminal justice purposes include adjudication, apprehension, correctional supervision, detection, detention, pre-trial release, post-trial release, prosecution, and rehabilitation of accused persons or criminal offenders. See 28 C.F.R.§ 20.3(b).

Criminal Justice Employment, Use Code "J": Also considered a criminal justice purpose, use code "J" is used by criminal justice agencies to screen employees or applicants for employment. See 28 C.F.R. § 20.21(b)(1) and 20.33(a)(1). N-DEx System users accessing the N-DEx System for criminal justice employment background checks must adhere to specific requirements relating to notice and consent, redress, and audits to protect the rights of the criminal justice applicant or employee.

Firearm-related Checks, Use Code "F": N-DEx System users may search the N-DEx System for the purpose of conducting a firearm, explosive, or associated license/permit background check. See 28 C.F.R. § 20.33(a)(5). The firearm-related checks must be conducted in accordance with the Brady Handgun Violence Prevention Act of 1993 (Brady Act) and implementing regulations set forth in 28 C.F.R. Part 25, Subpart A. This includes background checks for the transfer of firearms; the issuance of a firearm-related or an explosives-related permit or license (28 C.F.R. § 25.6 (j)(1)); inquiries by the Bureau of Alcohol, Tobacco, Firearms and Explosives in connection with a civil or criminal law enforcement activity relating to the Gun Control Act of 1968 or the National Firearms Act (28 C.F.R. § 25.6(j)(2)); and disposing of firearms in the possession of federal, state, local or tribal criminal justice agencies (28 C.F.R. § 25.6(j)(3)). The N-DEx System will purge all Use Code "F" search criteria in adherence with 28 C.F.R. § 25.9(c) and 63 *Federal Register* 58304 (Oct. 30, 1998).

Federal Fitness/Suitability Checks, Use Code "S": Pursuant to Executive Order 13467, as amended by Executive Order 13746, the N-DEx System may be used by federal executive agencies to conduct

background checks on covered individuals. See also 28 C.F.R. § 20.33(a)(2). The Executive Order defines "covered individual" as "a person who performs, or who seeks to perform, work for or on behalf of the executive branch (*e.g.,* Federal employee, military member, or contractor), or otherwise interacts with the executive branch such that the individual must undergo vetting." Executive Order 13746(i). "Vetting" includes "the process by which covered individuals undergo investigation, evaluation, and adjudication of whether they are, and remain over time, suitable or fit for Federal employment, eligible to occupy a sensitive position, eligible for access to classified information, eligible to serve as a non-appropriated fund employee or a contractor, eligible to serve in the military, or authorized to be issued a Federal credential." Executive Order 13746(m). N-DEx System users accessing the N-DEx System for this purpose must adhere to specific requirements relating to notice and consent, redress, and audits to protect the rights of the covered individual.

Security Risk Assessments, Use Code "B": Use code "B" allows the FBI to search the N-DEx System when conducting security risk assessments. The Bioterrorism Preparedness and Response Act of 2002 ("Bioterrorism Act") (codified in part at 42 U.S.C. § 262a) restricts certain individuals from access to, use of, or transfer of select biological agents and toxins. Pursuant to the Bioterrorism Act's implementing regulations (42 C.F.R. § 73.10), the Attorney General is required to conduct security risk assessments on all individuals applying for access to select biological agents and toxins to determine if the individual is restricted from such access under 18 U.S.C. § 175b or 42 U.S.C. § 262a.

Administrative Use Code "A": Use code "A" is used for system administration purposes. Record-owning agencies or record submitters/aggregators select use code "A" to retrieve and display N-DEx System contributed records in association with performing the agency's data administration/management duty. A search conducted under use code "A" will only return the searching agency's own records. Responses for this purpose are not disseminated for any other reason.

Each agency accessing the N-DEx System is assigned an originating agency identifier (ORI). The agency's assigned ORI indicates its type of agency (e.g., law enforcement, probation, court, corrections). Access to N-DEx System information is controlled by data sharing rules, as described above. Data sharing rules can be configured by user type (i.e., dependent on ORI) and also by use code. For example, a submitting agency could make its data green for law enforcement ORIs when conducting a use code "C" search and red when law enforcement ORIs conduct a use code "F" search. Similarly, a submitting agency could make its data green for law enforcement ORIs conducting a use code "C" search and red for corrections ORIs conducting a use code "C" search. For system development purposes, limited CJIS Division's system developers, system administrators, and contractors supporting the N-DEx System may have role based privileged user access to some or all data in the N-DEx System. The N-DEx Program Office personnel also have access to some or all data in the N-DEx System as necessary to support the N-DEx program.

Information in the N-DEx System can be retrieved by authorized N-DEx System users by performing a query. The N-DEx System offers three different user connection methods for searching/retrieving N-DEx Data: LEEP, a direct identity provider (IdP)[6] connection to the N-DEx

[6] An IdP is defined as an organization/agency that creates, maintains, and vets information about each of its authorized users for LEEP access. The IdP performs user authentication each time an individual logs in to LEEP. The IdP also

System (legacy connections only), and a federated query via Web services.

LEEP provides access for both individual users and users authenticating through an IdP. Authentication via the LEEP ID allows individual users to access the N-DEx System Interface via LEEP. Authentication through an IdP is managed by the user agency and authenticates to the N-DEx System via the Security Assertion Markup Language version 2.0 (SAML 2.0) standard to allow large groups of users to connect to the N-DEx System Interface.

A direct IdP connection to N-DEx allows an agency to act as an IdP and to communicate with the N-DEx System using the SAML 2.0 standard for user authentication. Both parties establish a baseline of trust and interoperability by exchanging metadata files. A metadata file is an XML-based configuration file that contains pertinent information about an entity that allows it to trust another entity.

A federated query via a web services connection allows users to conduct an automatic search/return of N-DEx records. The N-DEx System uses the LEXS-SR standard for all web services (machine-to-machine) search applications and defines a common format for information sharing.

Information can be queried by name or other personal identifiers, as well as by incident type, modus operandi, or other relevant factors. Queries are performed only when a legitimate need exists. When conducting a query, N-DEx System users are required to select a use code and provide a search reason which coincides with the purpose of conducting their search. The N-DEx System includes a search engine similar to those offered on the Internet. This search engine improves search response times, provides more precise search results, and improves text and structured search capabilities. Prior to reliance or action upon or secondary dissemination of any N-DEx System information, N-DEx System users must satisfy the Authorized Use Requirement (confirming the terms of N-DEx System information use) and the Verification Requirement (verifying the completeness, timeliness, accuracy, and relevancy of N-DEx System information) through coordination with the record-owning agency.

N-DEx System users can subscribe to an N-DEx System search, person, or record and receive notifications. This functionality enables N-DEx System users to set a query to run on a repetitive basis to identify a particular item of interest, such as a particular incident report, and to be notified of any changes or updates to the incident report. Users can subscribe to search criteria to be notified if new records match the search and/or if another user conducts the same search; to a record to be notified whenever the document is updated, and/or when another user views the same record; or to a person entity composite[7] within the N-DEx System to be notified if records about a specific individual are added, updated, or if another user views the person entity composite. Subscriptions are set to expire after 180 days; however, users can renew their subscriptions. Subscriptions cannot be set for noncriminal justice searches (i.e., searches conducted under use codes "S," "B," or "F").

The N-DEx System provides users with a batch query functionality which allows a user to

---

assigns the current attributes about the individual for a given information technology session. These attributes are presented when the user accesses LEEP via a secure web browser session at a designated URL, which then allows users access to Service Providers, in this case the N-DEx System.

[7] A Person Entity composite is a collection of all information within the N-DEx System that pertains to a specific person identified in N-DEx System records.

upload up to thousands of search terms at one time and receive one consolidated response. Once created, batch queries can be saved and run again at a later time. Subsequently run batch queries will only return new records or records that have changed since the last batch query. The batch search capability allows users to find the same N-DEx information in less time when conducting searches on large volumes of information.

The N-DEx System also includes functionality which allows users to search by geographic location. Using the geographic location functionality, users can set search parameters to restrict queries to a specific geographic area by specifying areas on a map (radius circles or area polygons) or by parameters set in search screens. When a search is conducted using the geographic location functionality, only records contributed by agencies within the specified geographic area will be returned.

The N-DEx System will also retrieve and display records from connected systems through federated searches. N-DEx System users can retrieve records from federated data sources by selecting the federated data source during their search inquiry. Most federated searches require users to use targeted searches, which search for specific people, places, or things, as compared to simple searches which search for a keyword or phrase found anywhere on a document, regardless of context.

As referenced above, the N-DEx System connects with other federal, state, local, tribal, and territorial databases. Through federated searches, the N-DEx System provides users with the ability to search multiple data sets using one username and password. Federated searching involves data which is not collected or maintained within the N-DEx System. When an N-DEx System user conducts a federated search, the N-DEx System passes a search request transaction to another system, which in turn queries its database. The system then takes the results of the search request and provides them to the N-DEx System as a response message. The N-DEx System displays the response message in a standard format on the results screen, but N-DEx does not save these federated search results. As stated above, N-DEx System users can only retrieve information from most federated data sources using a targeted search. Federated databases may only be searched for criminal justice purposes and cannot be searched under use codes "F," "S," or "B." When accessing and using information from federated databases, N-DEx System users are required to abide by all legal and policy requirements governing the federated database. Within the context of the N-DEx System, federated searches refer to the capability to access CJIS Systems of Services and non-CJIS data sources.

Federated searches of other CJIS Systems are only available to N-DEx System users if the CJIS Systems Agency (CSA) authorizes this capability for its users. If authorized for an N-DEx System user, the user can federate a search to, and retrieve data from, the following FBI CJIS systems: the National Crime Information Center (NCIC), the Interstate Identification Index (III), and the Next Generation Identification System (NGI). The N-DEx System makes automatic queries of the CJIS Systems, but the N-DEx System does not retain the information from the systems.

Non-CJIS criminal justice data sources to which the N-DEx System currently federates a search include the Department of Homeland Security's (DHS's) TECS database and its Enforcement Case Tracking System (ENFORCE); and the USNCB's INTERPOL database. To meet the criminal justice needs of its users, the N-DEx Program Office continually explores the ability to connect to other criminal justice information databases.

The N-DEx System has been approved through the CJIS Advisory Policy Board process to include federated searches of criminal intelligence databases, such as Texas Gang data and the Regional Information Sharing Systems Intelligence System (RISSIntel). As with information from the federated criminal justice databases, the criminal intelligence data will not reside or be contained within the N-DEx System. Only N-DEx System users possessing the required 28 C.F.R. Part 23 certification are permitted federated access to criminal intelligence information via the N-DEx System.

In addition to federated searches to other systems, the N-DEx System connects with other systems that search into, and retrieve information from, the N-DEx System. The Naval Criminal Investigative Service's Law Enforcement Information Exchange System (LInX), RISSIntel, the El Paso Intelligence Center (EPIC), and the Forensic Logic COPLINK systems are some of the systems that currently federate searches to N-DEx System data. For Use Code "F" purposes, the National Instant Criminal Background Check System (NICS) is developing the ability to connect to the N-DEx System and retrieve N-DEx System records matching the biographical data sent from NICS.

For information technology (IT) infrastructure purposes, the N-DEx System relies upon CJIS' Common Compute Platform (CCP), Enterprise Storage Services (ESS), Enterprise Web Services (EWS), CJIS Shared Enterprise Network (SEN), FBI's Cloud Network Services Environment (CNSE), the LEEP identity management tool, and the Amazon Web Services Government Cloud Environment (AWS GovCloud).

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 the N-DEx System will not be released for open data purposes or for research or statistical analysis purposes. Only authorized users, as discussed above, have access to the N-DEx System.

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.

With the exceptions identified below, in general, individuals who are subjects or targets of criminal investigations are not provided notice of this fact. A general notice of the existence of the N-DEx System and the types of records contained therein has been provided through publication of a System of Records Notice (SORN) in the Federal Register and through the publication of the initial PIA, which further described the N-DEx System. Additional general notice is provided by this PIA. Specific notice and consent are provided to individuals when the N-DEx System is used for criminal justice employment background checks, vetting conducted by federal executive agencies pursuant to Executive Order 13467 as amended by Executive Order 13746, or security risk assessments. In addition, individuals undergoing firearm-related checks are informed that their information will be used to determine if they are prohibited by law from possessing or receiving a firearm, explosive, or

related permit, which includes checking criminal justice information. As indicated above, however, such personal individualized notice is the exception and not the rule.

Contributors to the N-DEx System are criminal justice entities who have gathered the information for legitimate law enforcement or criminal justice purposes, such as incident, arrest, or parole and probation records. Because of the nature of the information contributed to the N-DEx System, notice is not provided to individuals whose information may be included within the N-DEx System.

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.

With the exceptions identified in the next paragraph, individuals are not provided the opportunity to consent to collection of information that pertains to them. Contributors to the N-DEx System are criminal justice entities who have gathered the information for legitimate law enforcement or criminal justice purposes, such as incident, arrest, or parole and probation records. Because of the nature of the information contributed to the N-DEx System, individuals do not have the opportunity to decline to provide it.

Individuals have the opportunity to consent to use of the N-DEx System for criminal justice employment, security risk assessment, or federal background check purposes. Individuals undergoing firearm-related checks are informed that their information will be used to determine if they are prohibited by law from possessing or receiving a firearm, explosive, or related permit.

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.

Generally, individuals do not have the ability to access or amend information in the N-DEx System. N-DEx System information is criminal justice information provided by criminal justice agencies for criminal justice use. Allowing individuals to access information collected and used for criminal justice investigations could alert the subject of an investigation of the fact and nature of the investigation, and/or the investigative interest of the FBI and other law enforcement agencies, or interfere with the overall law enforcement process. Amendment of these records could similarly interfere with ongoing investigations and other law enforcement activities and impose an impossible administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

However, agencies using the N-DEx System for employment and vetting purposes must provide the applicant with an opportunity to challenge and/or correct records if adverse action is taken based on information obtained from the N-DEx System. Individuals undergoing a firearm-related check may challenge the accuracy of a record upon which they are denied a firearm, explosive, or related permit through the procedures set forth in 28 C.F.R. § 25.10. Individuals undergoing a security risk assessment may challenge the decision to restrict their access to select biological agents or toxins through the procedures set forth in 42 U.S.C. § 262a and 42 C.F.R. § 73.20.

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):** The N-DEx System received its most recent ATO on June 21, 2022, with approval for continuous monitoring. Its next review date is June 23, 2023. **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:** The security controls applied to the N-DEx System are commensurate with the potential impact on the organizational operations, organizational assets, and individuals should there be a loss of confidentiality, integrity, or availability.
	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	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The N-DEx Program Office uses a security test and evaluation plan which validates system compliance with established security requirements and is one of the many security reviews conducted on the N-DEx System.
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:** N-DEx System user activity audit logs maintain a record of individual use of the N-DEx System, including the reason for the user's query. This facilitates spot audits to gauge compliance with the use of information in accordance with the N-DEx System and agencies' specific policies and/or agreements. These audit logs also are used as part of the overall N-DEx System audit to ensure proper use of information in compliance with FBI CJIS Division policies and agreements. The N-DEx Program Office has also established an N-DEx Auditor/Security Administrator capability which provides the ability to perform all audit modification procedures such as adding, removing, replacing, or delegating audit authority. In addition, criminal justice agencies are required to have audit and accountability controls in place.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.

X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** As discussed above, the N-DEx System provides a variety of computer-based trainings to assist users with N-DEx System functionality.

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?

Unauthorized or inappropriate access to N-DEx System information constitutes a threat to the functionality of the system, as well as to the privacy of those whose personal information is contained therein. Mitigation of this potential security and privacy risk relies on system controls that ensure that only authorized users have access to the N-DEx System. N-DEx System access is limited to criminal justice agencies, agencies performing the administration of criminal justice as defined by regulation, and federal executive agencies authorized to conduct vetting as set forth in Executive Order 13467 as amended by Executive Order 13746. Agencies have access to the N-DEx System only if they have an assigned ORI and agree to adhere to the *CJIS Security Policy* (available here: http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view). Each agency may only access the types of information for the purposes that have been authorized for its ORI. Such role-based access is strictly controlled and audited by the CJIS Division. The CJIS Security Officer (CSO) for each participating agency signs a CJIS user agreement acknowledging the CSA's obligations to ensure N-DEx System data is accessed, retained, and disseminated appropriately. Each CSO, in turn, ensures all N-DEx System users within his/her jurisdiction abide by the security requirements. All users must comply with applicable security and privacy protocols addressed in the *CJIS Security Policy*, the CJIS User Agreement, and the N-DEx System Policy. In accordance with the *CJIS Security Policy*, each CSO must sign a User Agreement with the CJIS Division and each record-owning agency must sign an Information Exchange Agreement with the CSO before exchanging information in the N-DEx System. Both record-owning agencies and N-DEx System users acknowledge that they understand sanctions may be applied for intentional misuse of the N-DEx System. The risk of unauthorized or inappropriate access is further mitigated through security awareness training and by periodic audits conducted by each CSO and the FBI to ensure N-DEx System searches are necessary and relevant to the user's official duties.

The privacy risk of unauthorized or inappropriate access to N-DEx System information is further mitigated by the N-DEx System's user training and audit management tools. CSOs are responsible for ensuring an N-DEx Agency Coordinator (NAC) is designated for each agency that accesses the N-DEx System and serves as the point of contact for the CSO. The audit management tools enable the CSOs and/or NACs to manage user privileges, access, and data sources within the N-DEx System. In addition, the N-DEx System requires a user to provide the following user identifiers prior to accessing the N-DEx System: Identity Provider ID, User ID, Last Name, First Name, and employer's ORI. These identifiers provide the N-DEx System and CSOs with the necessary elements to ensure only authorized and appropriate users are accessing the N-DEx System.

The N-DEx System password protection identification features and other system protection methods restrict access to information in the N-DEx System to enhance security and privacy. Warning banners regarding security and privacy are displayed on the N-DEx System to remind users about unauthorized disclosure of the information. Other data security and quality measures include: computer rejection of records with errors; automated data inspection prior to ingestion; and manual quality control checks by FBI personnel. In addition, data submitted to the N-DEx System from the FBI must follow an FBI Corporate Policy Directive which requires a phased security protocol consisting of both automated and manual data review processes to ensure that only appropriate unclassified FBI data is placed in the N-DEx System.

All N-DEx System users must be trained on the N-DEx System, with emphasis on data use rules, prior to accessing the N-DEx System. This requirement is achieved by users reviewing and agreeing to the N-DEx Data Access Agreement on an annual basis. Furthermore, the N-DEx Program Office makes available to participating agencies training resources regarding the requirements of N-DEx System access and the appropriate uses of N-DEx System data. In addition, all FBI employees and contractor personnel must complete annual information security and privacy training. This required training addresses the roles and responsibilities of the users of FBI systems and raises awareness of the sensitivity of the information contained therein and how it must be handled to protect privacy and civil liberties.

Finally, all users are subject to periodic on-site or remote audits conducted by both a user's own oversight entity and the CJIS Audit Unit. The audits assess and evaluate users' compliance with CJIS technical security policies, regulations, laws, and terms in the *CJIS Security Policy*, the CJIS User Agreement, and the N-DEx System Policy. N-DEx System user activity audit logs were built according to FBI CJIS Division standards and display N-DEx System user activities including the reason for the user's query. Deficiencies identified during audits are reported to the appropriate CSO and the CJIS Advisory Policy Board. Participation and access to the N-DEx System may be terminated for improper access, use, or dissemination of N-DEx System records. In addition, each Information System Security Officer (ISSO) is responsible for ensuring operational security is maintained on a day-to-day basis. Adherence to roles and rules is tested as part of the security certification and accreditation process.

The N-DEx Operations Team (OPS), ISSOs, and System Security Administrators (SSAs) continually review the security controls as required by the FBI Security Assessment and Authorization Policy Guide and also use National Institute of Standards and Technology (NIST) Special Publication 800-53 for expanded definition and guidance. The N-DEx System is a FISMA reporting system and the ISSO is required to review security controls and complete reports annually. Security Control Risk Assessment 5 (RA-5) focuses on assessing risk to reduce the risk of unauthorized access, use, and disclosure. The risk assessment is reviewed and updated at least annually. The Security Impact Level for Confidentiality is moderate, and confidentiality is protected through NIST security controls, including, but not limited to, NIST requirements for boundary protection/external communications services (SC-7[4]), transmission confidentiality and integrity (SC-8), access controls for remote access (AC-17[2]), and media transport protections (MP-5[4]).

The FBI hosts portions of the N-DEx System in the physically secure CJIS Common Operating Environment (COE) and CCP. Additional N-DEx workloads are hosted in the AWS GovCloud, which has reached FedRamp High approval. All N-DEx System components in the AWS GovCloud reside

in FBI-controlled virtual private clouds. N-DEx System data is logically separated from other systems. All communications between the FBI on premises infrastructure and the cloud service provider will be encrypted in transit using the FBI's CNSE. All N-DEx data stored in AWS GovCloud is encrypted at rest.

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.)

The National Archives and Records Administration (NARA) has approved the destruction of FBI-contributed data to the N-DEx System after a period of 25 years, see NARA Job No. N1-065-11-2. Audit logs must be maintained for 25 years or, in the event of a dissemination of information from the N-DEx System, the life of the record, whichever is longer. Contributed records in the N-DEx System are maintained and disposed of in accordance with the record retention schedule(s) applicable to the record-owning agency. In addition, the N-DEx System shall purge all firearm-related search criteria in adherence with 28 C.F.R. § 25.9(c) and 63 *Federal Register* 58304 (Oct. 30, 1998).

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:

National Data Exchange (N-DEx) System, JUSTICE/FBI-020, 83 Fed. Reg. 64601 (Dec. 17, 2018) available at: https://www.justice.gov/opcl/page/file/1191931/download

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.***

As discussed above, the N-DEx System contains criminal justice information submitted by criminal justice agencies including arrest, booking, incarceration, parole, and probation records. A privacy risk may exist due to the enhanced sharing of this data in the N-DEx System. Data about crimes and criminal incidents, which are already collected by criminal justice agencies as part of their legally authorized missions and which were previously functionally obscure, will now be more readily apparent and retrievable. Therefore, the cumulative effect on individual privacy is that N-DEx System users will potentially have access to more information about suspected offenders, witnesses, or victims from related criminal justice incidents or events involving those same individuals. The advantage for N-DEx System users is the ability to draw from this linkage a more complete, and far more timely, investigative analysis which should, in turn, lead to a more effective and efficient resolution of the investigation. This enhanced ability to solve crimes, identify perpetrators, eliminate misidentification of the innocent, and assist victims - coupled with the capability of the N-DEx System to robustly monitor information sharing practices - far outweighs any cumulative impact on the privacy of individuals whose information is already lawfully included in criminal justice records throughout the country. Moreover, this information has been available to and shareable by the FBI for several years; the N-DEx System simply provides an automated means to make it available to other criminal justice partners. User access to the information is always subject to the CJIS Division and N-DEx System security and policy restrictions which permit access to information for a criminal justice, or limited noncriminal justice, purpose and require users to enter a use code and reason for each query. All searches are subject to auditing. In addition, as discussed above, submitters of the information can control access to the data they add to the system.

Information collected for criminal justice purposes may present a privacy risk of "over-collection" because it is often difficult or even impossible to determine what information will be ultimately relevant to an investigation. The N-DEx Program Office has mitigated this risk by requiring all entities accessing the N-DEx System, and all information placed in the N-DEx System, to comply with the requirements of the *N-DEx System Policy and Operating Manual* (available at: https://www.fbi.gov/services/cjis/ndex/). The N-DEx System policy emphasizes that each criminal justice entity using the N-DEx System is responsible for compliance with its own rules and authorities. Consequently, information contributed to the N-DEx System can only be shared based on legal authority. The Policy also requires data contributors, at least every 30 days, to ensure that their records are up to date. When an agency updates records in its own system, it is required to make a corresponding update to the records contributed to the N-DEx System. The N-DEx System is able to generate reports to show how often an agency modifies or deletes its records; therefore, this functionality is auditable. Finally, before any user takes action based on records contained in the N-DEx System, the N-DEx System authorized use and verification policy requires the record-requesting agency to contact the record-owning agency and verify that the records are complete, timely, accurate, and relevant. N-DEx System information may not be used as a basis for action or further disseminated outside the participating agency that accessed the information, unless the agency first obtains the permission of the record-owning agency or unless an actual or potential threat of criminal activity or terrorism exists, as described in N-DEx System policy. This advanced use and verification policy helps to ensure the underlying information can be verified and updated as necessary before action is taken. The authorized use and verification policy specifically prohibits inclusion of

the N-DEx System information in an official investigative or case file and any use of N-DEx System information in the preparation of judicial process such as affidavits, warrants, or subpoenas without advanced permission of the record-owning agency.

A privacy risk can result from placing sensitive information, which includes PII of victims and witnesses, into a national information sharing system like the N-DEx System because this could lead to overly broad access to the information. In mitigation, the N-DEx System provides participating agencies with configurable tools that enable record-owning agencies to control the dissemination of their more sensitive information. The tools allow data owners to set the sharing rules for their records. Only individuals designated as a Source Data Administrator (SDA) by the contributing agency's CSO or NAC have access to the configurable tools. Data contributors may further tailor the levels of sharing according to the type of N-DEx System user by restricting data access to specific agencies or groups based on ORI.

Data shared in the N-DEx System may present a privacy risk because it could be inaccurate or outdated. An offender/arrestee may provide a range of information throughout the criminal justice process often with varying degrees of veracity. However, all of the information the arrestee/offender provides may have law enforcement value. The risk of inaccurate or outdated information is mitigated by the fact that the N-DEx System information must be verified with the record-owning agency, as noted above. This risk is further mitigated by the requirement that record-owning agencies periodically update their records. The N-DEx Program Office, through the CJIS Division's Advisory Process, has established a policy requiring each data contributor to maintain "system discipline." Each data contributor must maintain timely, accurate, and complete information in the N-DEx System. In an effort to maintain system discipline, contributors shall submit data, including any updates or changes to the original submission, on at least a monthly basis. Compliance with this policy, consistent with long-standing CJIS Division user agreements and the CJIS Audit Unit policy, are part of an audit program for the N-DEx System. The CAU conducts audits of state and federal CSAs once every three years. The audits include a review of access to CJIS systems (e.g., NCIC, N-DEx) by the CSA and any local agencies under the CSA's oversight or which receive CJIS access through the CSA. N-DEx System audits consist of: an administrative interview of the NAC; network inspection; a review of random N-DEx System transactions; a review of user access; technical security; and NCIC and III policies (if the agency's users can access NCIC and III from the N-DEx System). The CAU's N-DEx Audit Program does not include a data quality review component; however, it is in the interests of the criminal justice community to keep records as complete, timely, accurate, and relevant as possible in order to effectively accomplish its mission. The N-DEx System is designed to provide criminal justice agencies with sufficient access to ensure all data they submit is accurate, timely, and complete. Auditing capabilities, nevertheless, allow usage of the N-DEx System to be tracked, regardless of user role or access level. These policies and practices, along with the ability to limit dissemination of sensitive information, ensure the protection of data in the system.

There is also a risk that information within the N-DEx System may be stale or inaccurate. To mitigate this risk, data submitters have an obligation to ensure the information provided is reasonably accurate, timely, relevant, and complete. Records can be purged upon request of the submitter. Although the maximum retention period for N-DEx System records is 25 years, the information can be purged before that period elapses, depending on the needs of the submitting record holder.

Finally, the privacy of criminal justice applicants, firearm applicants, individuals applying for

access to select biological agents and toxins, and covered individuals vetted by federal executive agencies may be compromised when an agency searches the N-DEx System as part of an employment, firearm-related, security risk assessment, or federal background check. To mitigate this risk, before searching the N-DEx System for an employment, security risk assessment, or federal background check purpose, the agency must provide notice to the applicant, and the applicant must return a written consent. The applicant's concurrence to the N-DEx System search for the employment, security risk assessment, or federal background check must be documented in the applicant's file. Individuals undergoing firearm-related checks are informed that their information will be used to determine if they are prohibited by law from possessing or receiving a firearm, explosive, or related permit. To assist with auditing the use of the N-DEx System for employment, vetting, security risk assessment, or firearm-related purposes, the N-DEx System user must enter a specific use code which identifies the purpose of its search. As discussed in Section 4 above, agencies contributing data to the N-DEx System may choose not to permit searching of their records for employment, vetting, security risk assessment, or firearm-related purposes. Agencies using the N-DEx System for employment and vetting purposes must also provide the applicant with an opportunity to challenge and/or correct records if adverse action is taken based on information obtained from the N-DEx System. Individuals undergoing a firearm-related check may challenge the accuracy of a record upon which they are denied a firearm, explosive, or related permit through the procedures set forth in 28 C.F.R. § 25.10. Individuals undergoing a security risk assessment may challenge the decision to restrict their access to select biological agents or toxins through the procedures set forth in 42 U.S.C. § 262a and 42 C.F.R. §73.20. In addition, PII in the search criteria for noncriminal justice searches conducted under use codes "F," "B," and "S" is redacted from the audit logs, and subscription and notification capabilities are disabled for use codes "F," "B," and "S." This ensures that criminal justice users are unaware of the individuals being searched through the N-DEx System for noncriminal justice purposes. These additional safeguards work in conjunction with the other N-DEx System requirements to protect an applicant's privacy and due process rights.