Federal Bureau of Investigation

Privacy Impact Assessment
for the
National Crime Information Center

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: November 7, 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 Crime Information Center (NCIC) is a national criminal justice information system linking criminal (and authorized noncriminal) justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, and select foreign countries to facilitate the cooperative sharing of criminal justice information. The Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division operates the NCIC. The NCIC's mission is to provide a timely and accurate database of current criminal justice information available to authorized criminal justice personnel 24 hours a day, 365 days a year. More information about the NCIC is available online at <https://www.fbi.gov/services/cjis/ncic.>

The last major upgrade to the NCIC occurred in July 1999, with the implementation of NCIC 2000. In order to accommodate NCIC user requirements, the FBI CJIS Division has implemented many operational and technical enhancements to the system since the rollout of NCIC 2000. As the lifecycle of the technology deployed in NCIC 2000 nears its end, the FBI CJIS Division is preparing for the next major upgrade to NCIC, known as NCIC Third Generation (N3G). The purpose of the N3G project is to identify requirements that will improve, modernize, and expand the existing NCIC system so it will continue to provide real-time, accurate, and complete criminal justice information that will support law enforcement and criminal justice communities. This Privacy Impact Assessment (PIA) revises the previously published PIA for NCIC, incorporating the changes made by N3G, while still providing an overview of the types of personally identifiable information (PII) contained in the NCIC and the use of the information to further criminal justice objectives.

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 NCIC is a computerized information system containing documented criminal justice information that is searched by name and other descriptive data. The FBI established the NCIC system in 1967 as a service to facilitate the sharing of law enforcement information, and participation now encompasses criminal and authorized noncriminal justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, and select foreign countries. The NCIC provides a system to receive and maintain information contributed by participating agencies relating to criminal justice and national security missions. The NCIC now includes an extensive collection of criminal justice information that can be accessed electronically by, and furnished to, any authorized user terminal without the need for manual processing by the FBI. The NCIC contains a variety of files

consisting of records contributed by participating criminal justice and authorized noncriminal justice agencies.

The goal of the NCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information described in Section 3 below. Through the CJIS Advisory Policy Board, members of the criminal justice community make recommendations to the Director of the FBI concerning the philosophy, concept, and operational principles of the NCIC System. Information maintained in the NCIC is readily accessible for authorized purposes by authorized users via text-based queries (i.e., using names and other descriptive data). Authorized purposes include apprehending fugitives; solving crimes; combating acts of terrorism; locating missing persons; locating and returning stolen property; protecting individuals during declared emergency situations; protecting victims of domestic violence; monitoring registered sex offenders; conducting firearm, explosive, and weapons related permit background checks; and enhancing the safety of law enforcement officers. NCIC also maintains information about individuals required by statute, executive authority, or other legal authority to undergo continuous re-vetting to maintain employment or security clearance with a federal agency and information about individuals who have provided their information to federal agencies for the purposes of immigration benefits or other government benefits which require ongoing suitability determinations. NCIC authorized users enter records into the NCIC, which, in turn, are accessible to authorized agencies nationwide and select foreign agencies. The NCIC queries allow authorized agencies quickly and efficiently to receive criminal justice information about individuals they encounter while performing their criminal justice and national security missions.

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; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat 272; the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat 3638; the Implementing Regulations of the 9/11 Commission Act of 2007, Pub. L. 110-53, 121 Stat 266
X	Executive Order	13311, 13356, 13388
X	Federal Regulation	28 CFR § 0.85, part 20, and § 50.12
X	Memorandum of Understanding/agreement	Memorandum of Cooperation between the Royal Canadian Mounted Police and the Federal Bureau of Investigation Regarding the Direct Automated CPIC/NCIC Interface (2015 latest version)

	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.

The NCIC contains a variety of law enforcement sensitive files and other information. The NCIC has specific requirements for which agencies may enter records into a file, the necessary data elements for each record, and which agencies may access the file. These requirements vary based on the data content of each NCIC file. Criminal justice and authorized noncriminal justice agencies utilize information contained in these files as authorized to meet their needs. Agencies that enter records remain responsible for the accuracy, timeliness, and completeness of those records. Requirements concerning which agencies can make entries and what data elements are required for specific entries vary according to the nature of the file.

NCIC files are divided into two categories, Persons Files and Property Files, and contain the following information:

1. NCIC Persons Files

The following files maintained in the NCIC may contain some or all of the following descriptors and biographical information regarding individuals in the database: name; gender; race; place of birth; date of birth; height; weight; eye color; hair color; FBI number or universal control number (UCN);[1] skin tone; scars, marks, and tattoos; miscellaneous numbers (MNU);[2] Social Security number; driver's license number and issuing state; license plate number and issuing state; passport information; deoxyribonucleic acid (DNA) profile indicators signifying whether a criminal justice agency has an individual's DNA; addresses; country of citizenship; ethnicity; aliases; e-mail addresses and other internet identifiers; employer name; fingerprint classification information; state identification number; telephone numbers; photographs; and physical and medical characteristics or other personal information necessary to identify an individual, protect law enforcement officers, and protect law enforcement subjects. Generally, all criminal justice agencies can enter records into and retrieve records from the NCIC person files consistent with the rules of the system.

[1] The FBI Number/UCN is a unique identification number assigned to each identity in the Next Generation Identification (NGI) system.
[2] An MNU is any unique identifying number assigned to the subject of an NCIC record by a contributing agency such as a military number or a state identification number.

Wanted Person File

The Wanted Person File contains records of individuals who have outstanding arrest warrants. This File also contains records of juveniles who have been adjudicated delinquent and who have escaped from custody or supervision or who have absconded while on probation or parole. The File also contains records of juveniles who were charged with committing an act of delinquency that would be a crime if committed by an adult and who have fled from the state in which the act was committed. Agencies may also enter temporary "felony want records" into this File. Temporary felony want records allow a law enforcement agency to take prompt action to apprehend a person suspected of committing a felony when circumstances prevent the agency from immediately obtaining a warrant. Temporary felony wants are automatically retired 48 hours after entry. Only authorized law enforcement/criminal justice agencies may enter records into this file; however, the National Center for Missing and Exploited Children (NCMEC) can indicate an investigative interest in a wanted person record. NCMEC can also append images to a Wanted Person record.

Missing Person File

The Missing Person File contains records of missing persons of any age who have a proven physical or mental disability; records of persons who are missing under circumstances indicating that they may be in physical danger or abducted; records of persons missing after a catastrophe; records of persons under the age of 21 who are missing but who do not meet any of the above criteria; and records of persons aged 21 and older who are missing, who do not meet any of the above criteria, but for whom there is a reasonable concern for their safety. This file also contains records of persons with information about the missing persons. Only authorized law enforcement/criminal justice agencies may enter records into this file; however, the NCMEC can update records in this File to indicate it has an investigative interest in a missing person. NCMEC can also append images to a Missing Person record.

Foreign Fugitive File

The Foreign Fugitive File contains records from the International Criminal Police Organization (INTERPOL) and the Royal Canadian Mounted Police (RCMP). INTERPOL records within the Foreign Fugitive File contain information on persons wanted in other countries for crimes that would be felonies if committed in the United States. The wanting country must have signed an extradition treaty or convention with the United States, or the subject must be wanted for a violent crime or otherwise must be known to be violent, armed, or dangerous. The RCMP records within the Foreign Fugitive File contain information on persons who are wanted for violations of the Criminal Code of Canada and for whom there is an outstanding Canada-wide warrant. Only the staff of INTERPOL's United States National Central Bureau (USNCB) and the RCMP can enter records into this File.

Immigration Violator File

The Immigration Violator File contains records of criminal aliens whom U.S. immigration authorities deported for drug or firearms trafficking, serious violent crimes, or both; information on aliens who have outstanding administrative warrants for removal from the United States and who have unlawfully remained in the United States; and records of aliens who have outstanding administrative warrants for failure to comply with national security registration requirements. Only the Department of Homeland Security's Bureau of Immigration and Customs Enforcement can enter records into the Immigration Violator File.

Protection Order File

The Protection Order File contains records of individuals who are subject to court-issued orders to prevent violent or threatening acts, harassment against, contact or communication with, or physical proximity to another person(s). The Protection Order File also contains information about the protected person(s) for whom the court order was issued and terms and conditions of the protection order. Only authorized law enforcement/criminal justice agencies and civil courts involved in domestic violence and stalking cases may enter records into this file.

Extreme Risk Protection Order (ERPO) File

The ERPO File contains information about individuals subject to orders issued by a criminal or civil court temporarily restricting an individual from purchasing or possessing a firearm, ammunition, or other related items, based on a finding that they may pose a significant danger of personal injury to themselves or others. The ERPO File may also include the name of the individual petitioning for the ERPO. Only authorized law enforcement/criminal justice agencies may enter records into this file.

National Sex Offender Registry (NSOR)

The NSOR contains records of sex offenders or other persons required to register under a federal, state, local, or tribal jurisdiction's sex offender registry program. Only authorized law enforcement/criminal justice agencies may enter records into this file.

Supervised Release File

The Supervised Release File contains records of individuals who are under specific restrictions during their probation, parole, supervised release, or pre-trial or pre-sentencing release. Only law enforcement/criminal justice agencies can enter records into this file. In addition to biographic descriptors about individuals under supervised release, this file contains conditions of the supervised release.

Identity Theft File

The Identity Theft File contains records of victims of identity theft with descriptive and other information that law enforcement personnel can use to determine if an individual is a victim of identity theft or if the individual might be using a false identity. Victims of identity theft voluntarily provide their information to law enforcement for entry into this file. Only law enforcement/criminal justice agencies may enter records into this file.

Gang File

The Gang File contains records of criminal gangs and their members. This information warns law enforcement officers of the potential danger posed by individuals and promotes the exchange of information about gangs and gang members to facilitate criminal investigations. To enter individuals into the gang file, a criminal justice agency must have developed sufficient information to establish membership or other relationship in a particular gang by either the individual's self-admission or pursuant to documented criteria. For NCIC purposes, a gang is defined as a group of three or more persons with a common interest, bond, or activity characterized by criminal activity or delinquent conduct. Only law enforcement/criminal justice agencies can enter records into the Gang File. Only law enforcement/criminal justice agencies can receive information from the Gang File.

Terrorist Screening Center (TSC) File

The TSC File contains records on individuals known or suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism; and national security threat actors, who are individuals assessed to be a threat to the safety, security, or national interest of the United States pursuant to Executive Order, Presidential Memorandum or Directive, Attorney General Order, or statute. The Terrorist Screening Center is the only entity that can enter and maintain records in this file, which is available to all law enforcement/criminal justice agencies.

Protective Interest File

The Protective Interest File contains records of individuals whom an authorized agency reasonably believes, based on its law enforcement investigation, might pose a threat to the physical safety of protectees or their immediate families. Only law enforcement agencies with a protective mission as specified within municipal, state, or federal statutes, regulations, or other appropriate legal authority may enter records into this File. The Protective Interest File expands upon the U.S. Secret Service Protective File that was originally created in 1983.

National Instant Criminal Background Check System (NICS) Denied Transaction File (NDTF)

The NDTF contains records about individuals who have been disqualified from possessing, transferring, or receiving firearms or explosives, or have been denied a weapons permit under applicable state or federal law pursuant to the NICS. NDTF records are entered and canceled through an interface between the NCIC and the NICS. Only the FBI's NICS Section can enter and maintain records in this file.

Violent Person File (VPF)

The VPF contains records of individuals who have been convicted of violent crimes against law enforcement, have made credible threats of violence against a member of the law enforcement or criminal justice community, have been convicted of a violent crime against a person, or have been convicted of a violent crime where a firearm or weapon was used. The VPF was designed to alert law enforcement officers that an individual they are encountering may have the propensity for violence against law enforcement. Only law enforcement agencies can enter records into the VPF.

Unidentified Person File

The Unidentified Person File contains records of unidentified deceased persons, living persons who are unable to ascertain their identities (e.g., amnesia victim, infant), unidentified catastrophe victims, and recovered body parts. Only law enforcement/criminal justice agencies may enter records into the Unidentified Person File; however, NCMEC can indicate an investigative interest in an unidentified person record. NCMEC can also append images to an Unidentified Person record.

Case Subject List

The Case Subject List includes biographical information on individuals who are or were, within the last five years, under investigation for a potential nexus to terrorism. Only the FBI can enter records into and receive a query result from this file.

2. NCIC Property Files

The following Files contain information about property. These files may include PII and other data elements that might be traced back to an individual, such as vehicle identification number, license plate number, serial number, and information about the property owner, such as name, as well as an owner applied number, which is a number that is provided by a person for a vehicle which the person built. All NCIC Files include a miscellaneous field that can be filled with any information, including additional PII. Generally, all law enforcement/criminal justice agencies can enter records into the property files.

Article File

The Article File contains records of any stolen item valued at $500 or more; records of all property taken, regardless of value, if the aggregate value taken in one theft exceeds $5,000; records of property taken, regardless of value, if the investigation indicates interstate movement of the property; records of property taken in which the seriousness of the crime indicates that the investigating agency should enter a record for investigative purposes; or records of lost Public Safety, Homeland Security, or Critical Infrastructure items of identification. Information in the Article File includes the brand name, model, serial number, and an owner applied number (if applicable) of the property listed. Only law enforcement/criminal justice agencies can enter records into the Article File.

Gun File[3]

The Gun File contains records of stolen weapons; recovered (abandoned, seized, or found) weapons; lost or missing weapons; or weapons that have been used in the commission of a felony. Information in the Gun File includes the serial number, caliber, make, type, and model of the weapon listed, if available. Only criminal justice agencies can enter records into the Gun File.

License Plate File

The License Plate File contains records of stolen license plates. Information in the License Plate File includes the license plate number, the state in which the license plate was issued, the year the license plate was issued, and the type of license plate (e.g., passenger automobile, motorcycle, trailer, truck, aircraft, antique automobile, bus, commercial vehicle, dune buggy, farm vehicle). Only law enforcement/criminal justice agencies can enter records into the License Plate File.

Vehicle File

The Vehicle File contains records of stolen vehicles, vehicles used in the commission of a felony, or vehicles that a law enforcement agency seizes based upon a federally issued court order. Information in the Vehicle File includes the vehicle identification number, vehicle make, vehicle model, vehicle style, vehicle color, vehicle year, owner applied number (if applicable), and license plate number. Only law enforcement/criminal justice agencies can enter records into the Vehicle File.

---

[3] For NCIC purposes, a gun is defined as any weapon, including a starter gun, which is designed to or may be readily converted to expel a projectile by air, carbon dioxide, or the action of an explosive. Included in this definition are antique guns; cannons; machine guns; pistols; rifles; shotguns; the frame or receiver of any such weapon; any firearm muffler or firearm silencer; destructive devices such as grenades, mines, missiles, and rockets; and disguised guns such as knife guns, pen guns, belt buckles, and cane guns. Ball bearing (BB) guns are excluded and should be entered in the Article File.

Securities File

The Securities File contains records of securities that were stolen, embezzled, used for ransom, or counterfeited. Securities are identified as currency and documents or certificates that are evidence of debt or ownership of property or documents that represent subscription rights. Examples of securities include Federal Reserve notes, warehouse receipts, traveler's checks, money orders, stocks, and bonds. The following is mandatory information contained in this File: type of security, value amount of the security, serial number, the name of the issuer, and the name of the owner. The file may also include the date the security was issued, the owner's social security number, and whether the submitting agency has marked the security as being counterfeit or used for ransom or bait. Only law enforcement/criminal justice agencies can enter records into this File.

Boat File

The Boat File contains records of stolen boats. The File contains the following information: originating agency identifier, agency case number, date of theft, the make of the boat, and the year the boat was manufactured. Only law enforcement/criminal justice agencies can enter records into this File.

Vehicle/Boat Part File

The Vehicle/Boat Part File contains records of stolen component parts from a vehicle or boat or stolen ownership documentation such as titles. The file includes the following information: brand name, serial number, and owner applied number. Only law enforcement/criminal justice agencies can enter records into this file.

3. Other Files

Image File

Images can be associated with NCIC records to assist agencies in identifying people and property items. The Image File contains facial images related to people (such as mug shots, missing person, and passport photos); images of scars, marks, tattoos; and images of signatures. In addition, for reference, agencies can include images of property (e.g., vehicles, boats, guns). All images submitted to the Image File must be associated with a record in another NCIC file. Generally, only law enforcement/criminal justice agencies may enter records into the Image File; however, NCMEC can append images to records in the Missing Person, Wanted Person, and Unidentified Person Files.

Originating Agency Identifier (ORI) File

An ORI is a nine-character identifier assigned to an agency to identify the agency in transactions on CJIS systems. Agencies must have an ORI to access the NCIC. The ORI File contains contact information (such as an agency's address and telephone number) for agencies and their associated ORIs.

4. Other Information in the NCIC

In addition to active records in the designated files above, the NCIC maintains retired records, which are records removed from the active NCIC Files and not returned through general queries of the NCIC. Retired records are records that have been cleared, canceled, or have expired. An agency clears

or cancels a record when the purpose for entering the record has been resolved (e.g., a missing person has been found; a warrant has been executed; a stolen article has been recovered), or the record is inaccurate, invalid, or has been expunged. Expired records are records for which the retention period has expired or that have been removed from active status because they were not validated. Although retired records are still generally available to all NCIC authorized users for historical reference after the records have expired, cleared, or cancelled from the active NCIC files, they are only directly accessible and searchable by FBI personnel and CJIS Systems Agencies (CSAs).[4] For criminal justice purposes, general NCIC users may request that authorized FBI staff or CSAs search all retired records. Retired Records contain the same information as entries in active NCIC Files.

The Protection Order File and the National Sex Offender Registry also contain inactive records. Inactive records are a subset of retired records still accessible to authorized NCIC users via a direct query of the Protection Order File or National Sex Offender Registry. In the Protection Order File, inactive records are records for which the expiration date has passed, records which have not been validated, and records that have been cleared by the entering agency. The system maintains expired and cleared Protection Order File records in an inactive status for the remainder of the year in which the record was cleared or expired plus five years, after which they are retired and no longer generally accessible to NCIC users. Inactive records in the NSOR are records that have been cleared by the entering agency and expired records. Inactive records remain in the NSOR indefinitely unless they are cancelled by the entering agency. Once canceled, NSOR records are retired and no longer generally accessible to NCIC users. All authorized NCIC users may retrieve inactive records from the Protection Order File and the NSOR by directly querying the Protection Order File or the NSOR. A general query of the NCIC will not return inactive records from the NSOR or Protection Order File unless the query contains the NCIC number[5] assigned to the record.

The NCIC also maintains a copy of the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) Violent Felon File, which contains information on individuals with three or more convictions for a violent felony or serious drug offense as defined by 18 U.S.C. 924(e). This information, which was entered into the ATF Violent Felon File between 1992 and 1998, is held outside of the regular NCIC Files and is only directly available to FBI NCIC users and CSAs.

In addition to the specific files described above, the NCIC contains a series of tables and charts that are used for system administration purposes. The majority of the NCIC tables are comprised of data elements included in the above-described files. For example, the license plate table includes license plate number information from all the above files. However, certain tables also include biographic identifiers for individuals not contained in the above designated files. For instance, the investigative subjects of interest table includes subjects or vehicles associated with active FBI investigations. This table is maintained for internal FBI purposes. Only the FBI has access to this table.

---

[4] A CSA is a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the criminal justice information from various systems managed by the FBI CJIS Division. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS Systems.

[5] Also known as a "NIC" number, the NCIC number is a unique number assigned by the NCIC to each NCIC record.

The NCIC also maintains tables of individuals who are subject to continuous evaluation or who are subject to ongoing suitability determinations for federal benefits. These tables include individuals required by statute, executive authority, or other legal authority to undergo continuous re-vetting to maintain employment or security clearance with a federal agency. These tables also include individuals who have provided their information to federal agencies for the purposes of immigration benefits or other government benefits which require ongoing suitability determinations (*e.g.,* Trusted Traveler programs). Programs, such as Customs and Border Protection's Trusted Traveler Program, require their registered participants to be checked against the NCIC daily for new information that may impact one's eligibility in the program. Maintaining these tables within the NCIC lessens the administrative burden on federal agencies by automatically checking individuals required to undergo continuous evaluation or ongoing suitability determinations against added and updated NCIC information. The tables reduce the NCIC transaction workload of those queries that were being repeated daily.

Additional NCIC tables include information about individuals associated with the circumstances, investigation, and entering of NCIC records, such as governmental contacts, investigators, lab examiners, court and supervised release personnel, agency points-of-contact, law enforcement officers, and national security personnel.

The NCIC System also creates and maintains a Transaction Log, which the NCIC System Administrators monitor and review on a regular basis to detect misuse of system data and to trouble shoot system errors and problems. The Transaction Log contains all transactions that enter, update, query, or access the records described above; rejected transactions; and system administrative messages. Search criteria from transactions initiated by the NICS is not logged. Similarly, biographic descriptors from individuals subject to continuous evaluation are not maintained in the transaction logs. FBI staff can search the Transaction Log for validation, audit, misuse, and criminal justice purposes. Law enforcement/criminal justice agencies may request a search of the transaction log for active investigations.

The CJIS Division maintains two test environments for NCIC users to conduct testing of the NCIC. The first test system is for user training purposes only while the second system can be utilized for any type of testing whether for user training or for software development purposes. The testing environments do not contain actual NCIC data, only test transactions.

The chart below visibly depicts the types of information in the NCIC.

(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, and D	
Date of birth or age	X	A, B, C, and D	
Place of birth	X	A, B, C, and D	
Gender	X	A, B, C, and D	
Race, ethnicity or citizenship	X	A, B, C, and D	
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C, and D	
Tax Identification Number (TIN)			
Driver's license	X	A, B, C, and D	
Alien registration number	X	A, B, C, and D	
Passport number	X	A, B, C, and D	
Mother's maiden name			
Vehicle identifiers	X	A, B, C, and D	
Personal mailing address	X	A, B, C, and D	
Personal e-mail address	X	A, B, C, and D	
Personal phone number	X	A, B, C, and D	
Medical records number			
Medical notes or other medical or health information	X	A, B, C, and D	
Financial account information			
Applicant information	X	A, B, C, and D	
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, and D	
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents	X	A, B, C, and D	
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities	X	A, B, C, and D	

(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, and D	Records in the NCIC may contain information about criminal records in miscellaneous fields and may contain an individual's UCN, which links to criminal history records in the Next Generation Identification System (NGI); however, NCIC does not contain criminal rap sheets.
Juvenile criminal records information	X	A, B, C, and D	Records in the NCIC may contain information about criminal records in miscellaneous fields and may contain an individual's UCN, which links to criminal history records in NGI; however, NCIC does not contain criminal rap sheets.
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C, and D	The Missing Person File contains information about individuals associated with a missing person, which could include information concerning witnesses.
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			

(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
Biometric data:			The NCIC does not include biometrics, other than as listed below; however, the entries may include textual information indicating that subjects' biometrics are available in another system (e.g., fingerprints in the NGI; DNA or dental profiles available from a criminal justice agency).
- **Photographs or photographic identifiers**	X	A, B, C, and D	
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**	X	A, B, C, and D	
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:	X	A, B, C, and D	For NCIC transactions conducted for a NICS background check, only ORI, date/time of access, and queries run is retained. For all other system uses, the information below is captured.
- **User ID**			
- **User passwords/codes**			
- **IP address**			
- **Date/time of access**	X	A, B, C, and D	
- **Queries run**	X	A, B, C, and D	
- **Content of files accessed/reviewed**	X	A, B, C, and D	
- **Contents of files**	X	A, B, C, and D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):			MNU, Agency Case Number, License Plate Number, Vehicle Identification Number, State Identification Number; UCN. Other identifying numbers, such as an alien registration number, can be entered into the miscellaneous fields in NCIC as needed for criminal justice identification and use. Biographic descriptors such as height, weight, eye color, hair color, and skin tone. Additional information needed for criminal justice identification and use can be entered into the miscellaneous fields in NCIC.

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 NCIC does not collect information directly from individuals. All information is submitted by criminal justice or authorized noncriminal justice agencies.					

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

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): As discussed above, NCMEC may supplement some NCIC records.					

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	
DOJ Components			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			
Private sector	X			See narrative information below.

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.**
Foreign governments	X		X	Only Canada has direct access to the NCIC System. Other foreign governments may receive extracted information from the NCIC on a case-by-case basis. The exchange of NCIC information with foreign governments other than Canada is routed through DOJ's USNCB INTERPOL.
Foreign entities				
Other (specify):				

NCIC users generally access the NCIC through regional and/or state computer systems or, in some cases, through a direct line to the NCIC system. The NCIC provides a direct connection from one point of access in each State, U.S. Territory, Canada, the DOJ's USNCB INTERPOL, and authorized agencies. These access points are computers with NCIC dedicated routers directly wired to the NCIC through secure communication lines. The points of access are controlled and secured by the CSAs, which are required to ensure that access systems comply with the *CJIS Security Policy*. Some of the CSAs have disaster recovery sites that use internet connections under emergency conditions only. Authorized federal users may search NCIC via web interfaces available through the Law Enforcement Enterprise Portal (LEEP),[6] including the NCIC Mobile Service and Web Access Messaging Systems (WAMS). The NCIC Mobile Service, available to FBI personnel,[7] provides users the ability to remotely request information through the NCIC system to include person, vehicle, article, and gun queries. Through NCIC Mobile Service, users can also query Nlets data.[8] Users must become certified through their respective Terminal Agency Coordinator to use the NCIC Mobile Service. The NCIC Mobile Service allows users to query and receive NCIC information; however, users cannot enter, modify, cancel, or clear records via the NCIC Mobile Service. WAMS is a network that provides NCIC, Nlets, and Interstate Identification Index (III) access internally to various FBI divisions, task forces, and field offices. WAMS is the internal FBI user interface for users to send and receive NCIC message transactions, including queries of NCIC, and entering, modifying, clearing, and

[6] LEEP has separate privacy documentation.
[7] The NCIC Mobile Service is also available to the United States Marshals Service as a disaster recovery solution.
[8] The International Justice and Public Safety Information Sharing Network (also known as Nlets), is a nongovernmental, nonprofit agency which provides computer-controlled message switching to local, state, and federal agencies. Through the Nlets network, law enforcement and criminal justice agencies can access a wide range of state information, such as driver license and vehicle registration information, wildlife registration data, state warrant information, and state criminal history records. Nlets information is not housed within the NCIC, but the NCIC Mobile Service and WAMS allow users to query Nlets.

canceling NCIC records.

Agencies submit and retrieve records from the NCIC through a series of message keys. Message keys are codes designed to tell the NCIC what action should be taken with the information that is being submitted. For example, the message key "QWA" is used to conduct a search of all person files with the biographical information submitted. Other message keys are used for all functions of the NCIC such as to submit a record into certain NCIC files, to modify records, to clear records, and to send reject messages when a record does not meet the requirements for inclusion in a specific file. If a record-submitting agency sets a notification flag on its record, the record-submitting agency will receive an NCIC message whenever a search hits against its record. Similarly, agencies can use a message key to set an investigative interest in another agency's record.[9] If an agency sets an investigative interest in a record, they receive a notification anytime another agency's query hits against that record or the record is modified, canceled, or cleared.

The NCIC also includes a delayed inquiry function. Although all queries to the NCIC result in nearly immediate search results sent back to the inquirer, all queries (other than queries initiated by NICS) are also held in a delayed inquiry status for five days. If a record with information matching an inquiry's search terms is entered or modified within five days of the inquiry, the entering agency and the inquiring agency will receive notice that the record and inquiry contain matching data.

N3G enhancements include a query-query (QQ) capability allowing NCIC users to search a database of previous inquiries conducted in the NCIC System. The QQ functionality provides investigative benefit for agencies by allowing the user to determine if a specific person, vehicle, license plate, or property has been previously inquired upon in the last 30 days. Data returned from the QQ could potentially place a suspect or vehicle at the location of a crime scene. The QQ could also be used to locate a suspect during a critical case where locating the subject is time sensitive.

Information maintained in the NCIC is readily accessible for authorized purposes by authorized users via text-based queries (i.e., using names and other descriptive data). Authorized purposes for accessing the NCIC include apprehending fugitives, solving crimes, combating acts of terrorism, locating missing persons, locating and returning stolen property, protecting individuals during declared emergency situations, protecting victims of domestic violence, monitoring registered sex offenders, performing background checks for firearms, explosives, and weapon-related permits, and enhancing the safety of law enforcement officers. Not all NCIC users have access to all NCIC data. NCIC data is made available to different users in different ways, depending on the nature of the user and the nature of the data. Each using entity is assigned an ORI unique to the entity. Each using entity may only access the types of information for the purposes that have been authorized for the particular entity. Such access is strictly controlled and audited by CSAs and the CJIS Division.

FBI NCIC program users[10] have access to all information in the NCIC and can perform

---

[9] An agency can set an investigative interest in any record in an active NCIC file except for records in the NDTF, the Protective Interest File, the TSC File, and the Case Subject List.

[10] FBI NCIC program users include CJIS Division personnel in the Investigative and Operations Assistance Group (IOAG), and the NCIC Operations and Policy Unit (NOPU), Law Enforcement Support Section and Information Technology Management Section (ITMS) personnel supporting the NCIC.

"offline searches" of the NCIC. Offline searches are enhanced capability searches not limited to the specific retrieval parameters available to general NCIC users; rather, offline searches allow select users to retrieve information from the NCIC using any data field within the NCIC. NCIC system administrators have role-based access to the NCIC system to provide operational control, system administration, maintenance, and development of functions to support the NCIC operations. Access to select system tables and logs is further restricted to only a subset of authorized FBI users.

The CJIS Audit Unit (CAU) conducts compliance audits of CSAs and a sample of agencies serviced by each CSA, as well as ad hoc audits based on reports of violations. The CAU has access to all information in the NCIC.

In general, criminal justice agencies have read and write access to NCIC files, which may include the ability to make additions and changes to records they provided to the system. In contrast, noncriminal justice agencies and nongovernmental entities generally have limited access to the NCIC, such as query-only access to selected portions of the NCIC. Access to the records in the NCIC is determined by the user's FBI assigned ORI. All entities using the NCIC system are required to sign a user agreement agreeing to abide by the *CJIS Security Policy*. The CJIS Division's NCIC Operations and Policy Unit (NOPU) reviews requests for ORIs to access the NCIC under the authority of Title 28, United States Code, Section 534, and Title 28, Code of Federal Regulations (CFR) § 20.3(g) and § 20.3(b). Once received, NOPU reviews a request pursuant to federal law, regulations, and policies to determine if the requesting agency is eligible to access the NCIC. If the agency is eligible for access to the NCIC, NOPU assigns an ORI controlling the types of information the agency can access. All ORIs are validated on a biannual basis by the appropriate CSA to confirm all information associated with each ORI is current and accurate and to confirm the agency is still authorized to access the NCIC. There are two basic types of ORIs: full access and limited access.

Full Access ORIs may be granted to criminal justice and other authorized agencies for criminal justice purposes as defined in 28 CFR Part 20. Criminal justice agencies, as defined in 28 CFR § 20.3(g), include courts and any governmental agency (or subunit thereof) that 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.[11] The "administration of criminal justice" means the performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. The administration of criminal justice includes criminal identification activities and the collection, storage, and dissemination of criminal history record information. 28 CFR § 20.3(b). Criminal justice purposes also include screening visitors to critical infrastructure facilities, maintaining site security for criminal justice facilities and military installations, and performing background checks on employees/applicants for employment with criminal justice agencies. Examples of criminal justice agencies include local, state, tribal, federal, and Canadian law enforcement agencies, courts,[12] probation and parole, prosecutors, and correctional facilities.[13] Criminal justice and other authorized agencies with full access ORIs have read and write

[11] The phrase "allocates a substantial part" has been interpreted to mean more than 50 percent of an agency's annual budget.
[12] Courts that hear only civil cases are not considered criminal justice agencies.
[13] Facilities that house only juveniles who are not involved in the criminal justice process but who are orphaned or declared

access to NCIC Files, which includes the ability to enter and make additions and changes to records they provided to the system. Agencies can only modify records they provide to the NCIC.[14] Unless stated otherwise in Section 3 above, agencies with full access ORIs can access all information in the NCIC Files.

Noncriminal justice governmental agencies or private contractors which perform dispatching functions or data processing/information services for criminal justice agencies may also receive a full access ORI if they have an interagency agreement with a criminal justice agency or an executive order, statute, or regulation has delegated dispatching functions or data process/information services for a criminal justice agency to the noncriminal justice agency. *See* 28 CFR § 20.33(a)(6) and (7). In such cases, the noncriminal justice agency or private contractor has the same access as the criminal justice agency for which it is performing tasks. Governmental regional dispatch centers and nongovernmental railroad or campus police departments with arrest powers may also receive full access ORIs.

Limited Access ORIs are provided to authorized noncriminal justice agencies and authorized nongovernmental entities which have a need to access portions of the NCIC based on their responsibilities as defined in regulation or statute. Limited access ORIs provide access to selected portions of the NCIC based on the entities' needs. Examples of entities with limited access ORIs and the information they can access include:

Designated federal agencies required to complete security clearance background investigations under the Security Clearance Information Act, 5 U.S.C. 9101, have query access to all files in the NCIC. In addition, designated federal agencies may add individuals to the continuous evaluation table discussed in Section 3 above.

Governmental Social Service agencies with child protection responsibilities have query access to all the files in the NCIC. *See* Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248, section 151.

The NCMEC, a nongovernmental, noncriminal justice agency established by a government grant to aid the parents of missing and exploited children, has access to the Unidentified Person, Missing Person, Wanted Person, Image, and Vehicle Files. In addition to query access to these files, NCMEC can indicate an investigative interest in a wanted person, missing person, or unidentified person record. NCMEC can also append images to records in the Wanted Person, Missing Person, and Unidentified Person Files. *See* Adam Walsh Child Protection and Safety Act of 2006, Public Law 109-248.

Nongovernmental agencies (or subunits thereof) with regularly employed police officers with full police powers pursuant to state law and which allocate a substantial part of their annual budget to the administration of criminal justice, such as private campus, hospital, or railroad police departments, may have query and enter/modify access to the NCIC Protective Interest, Violent Person, Wanted Person, Missing Person, active Protection Order, and stolen property files.

---

incorrigible are not considered criminal justice agencies.

[14] The FBI creates all records in the ORI file; however, both the FBI and the agency assigned the ORI can update the agency information in the ORI file.

Governmental regional dispatch centers that provide communication services to criminal justice agencies may have query and enter/modify access to the Protective Interest, Violent Person, Wanted Person, Missing Person, active Protection Order, and stolen property files.

The National Insurance Crime Bureau, a nongovernmental, nonprofit agency that acts as a national clearing house for information on stolen vehicles, has limited access to the Vehicle, Boat, License Plate, and Vehicle/Boat Part files.

Noncriminal justice governmental department of motor vehicles or driver license registries with an essential need may have query access to the Wanted Person, Missing Person, Unidentified Person, License Plate, Vehicle, and Vehicle/Boat Part Files.

The International Justice and Public Safety Information Sharing Network (also known as Nlets), a nongovernmental, nonprofit agency which provides computer-controlled message switching to local, state, and federal agencies, has query access to the ORI file.

Civil courts have query and enter/modify access to the Wanted Person and Protection Order files for use in domestic violence and stalking cases.

Child support enforcement agencies have query only access to the Wanted Person, Missing Person, and Protection Order Files.

The United States Citizenship and Immigration Services has query access to all files in the NCIC except the ERPO File.

The Department of Justice's (DOJ) USNCB INTERPOL users have query and enter/modify access to the Foreign Fugitive File. They have query only access to all other NCIC Files. Through the USNCB INTERPOL, foreign INTERPOL National Central Bureaus (NCB) can query the NCIC; however, the only information returned is whether there is a potential match (red light/green light) to the information queried. Only the USNCB INTERPOL directly shares NCIC information with foreign INTERPOL NCBs.

Noncriminal justice medical examiners, coroners' offices, and state noncriminal justice missing person clearinghouses have query and enter/modify access to the Missing Person and Unidentified Person files.

Additional authorized agencies may receive access to select portions of NCIC as set forth in applicable laws. Any agency with an assigned ORI may query the ORI file. All agencies with an assigned ORI are subject to audit by their CSA and/or the CAU. The CAU conducts triennial NCIC audits of each CSA to include a sample of local agencies within its jurisdiction. The audit assesses the performance of the CSA in administering NCIC access and services. The CAU reviews the administrative policies and data quality procedures at the CSA and its local agencies. The CAU also conducts Information Technology (IT) Security audits to assess compliance with the *CJIS Security Policy* for agencies accessing NCIC. The *CJIS Security Policy* provides a baseline of security requirements including, but not limited to, personnel and physical security, access, use, and

dissemination for all CJIS systems. CSAs are also required to conduct triennial NCIC and IT Security audits of all agencies accessing NCIC within their jurisdiction.

CSAs assume responsibility for and enforce system security for all other agencies in a specific state or territory. CSAs are responsible for conducting their own compliance audits of the criminal and noncriminal justice agencies within the CSA's user community. CSAs have access to all active and inactive files. In addition, CSAs can retrieve retired records through offline searches.

In addition to the agencies described above that have direct access to the NCIC, the FBI also provides extracts of NCIC information to criminal justice agencies, private companies involved in the administration of criminal justice, and noncriminal justice and nongovernmental agencies with legal authority to receive certain portions of the NCIC records. Many criminal justice agencies receive an extract of NCIC information consisting of their own submitted records. Criminal justice agencies use the extracted information for system synchronization – to ensure that the records in the agency's system match the records the agency has submitted to the NCIC. Other entities receive extracts of specific NCIC files. For example, the U.S. Department of Housing of Urban Development receives an extract of the Wanted Person File twice a year and an extract of the NSOR file quarterly. To vet applicants for passports and visas, the Department of State receives a daily extract of the Wanted Person, Supervised Release, Missing Person, and Identity Theft files.

All agencies receiving an extract of NCIC information that is not used for system synchronization purposes sign a Memorandum of Understanding (MOU) with the FBI outlining what NCIC information will be provided, the permissible uses of the NCIC information, a requirement to abide by the NCIC hit confirmation policy, and requirements for disposal of stale NCIC data. Through the MOU process, the CJIS Division works with the FBI's Office of the General Counsel to ensure that the entity requesting an extract of the NCIC files is legally authorized to receive the NCIC information in accordance with federal law, regulations, and FBI policies. The CJIS Audit Unit has the authority to audit any entity that receives NCIC information to ensure the appropriate access, use, and dissemination of NCIC information.

As discussed above, direct access to retired records, the NCIC transaction log, and other information outside the designated NCIC Files is restricted to FBI NCIC users and CSAs. However, criminal justice agencies may request and receive this information from the FBI or their CSAs.

Interoperable systems may also search and return NCIC records to authorized users (i.e., users enter the query in a separate system which passes the query to NCIC). Users view the query results of NCIC searches conducted via interoperable systems in the interoperable system. For example, an authorized user could search NCIC information from the National Data Exchange System and have NCIC search results display within the National Data Exchange. Information within the NCIC can also be retrieved via the NICS and the NGI System via a secure, internal CJIS network. For example, if a user submits a fingerprint-based search on an individual to NGI, NGI will use the biographic information submitted with the fingerprints to query the NCIC. If the fingerprint submitter is authorized to receive NCIC records, NGI will return the NCIC results to the fingerprint submitter. If the biographic information submitted from NGI matches information in an NCIC record, the NCIC record owner also receives notification of the match.

The NCIC provides access to the NGI System through name-based queries of the III. The III is a name index which includes all individuals whose criminal history record information is maintained in the NGI. The III Program provides for the decentralized interstate exchange of Identity History Summary records, and functions as part of the NGI System. Only criminal justice agencies and agencies authorized by federal law may conduct named based searches of NGI via the III.

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.

The FBI does not release record information from the NCIC for open data purposes or for research or statistical analysis purposes. Only authorized users, as discussed above, have access to record information in the NCIC System. The FBI does publish and release NCIC Missing Person and Unidentified Person statistics on the fbi.gov website: https://www.fbi.gov/services/cjis/ncic.

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.

The FBI receives criminal justice information for the NCIC System from qualifying criminal justice and noncriminal justice agencies and entities rather than directly from the individuals to whom the information pertains. Agencies contributing information to the NCIC likely do not provide any sort of Privacy Act Statement or similar notice to the individuals about whom the information pertains. Non-federal contributors are not subject to the Privacy Act; federal contributors are usually exempted from the Privacy Act's individual notice provisions in connection with criminal law enforcement activities; and/or provision of individual notice incident to criminal law enforcement activities is typically impracticable. General notice regarding the collection of information in the NCIC has been provided to the public in the NCIC System of Records Notice. The publication of this privacy impact assessment (PIA) provides additional notice regarding the types of information maintained in the NCIC.

Additional notice might be provided by those agencies that contribute the underlying NCIC information. For example, PII for individuals included in the Identity Theft file is voluntarily provided to law enforcement for inclusion in the Identity Theft file. The FBI developed a consent form for agencies to use when collecting information for inclusion in the Identity Theft file. The consent form informs the identity theft victim of the purposes of providing the information and how the information may be used. However, agencies are not required to use the FBI provided consent form. Federal agencies providing information about individuals to the NCIC for benefits, employment, and security clearances provide such individuals with a Privacy Act statement informing them that their information will be provided to other governmental agencies and used to check criminal databases such as NCIC. Individuals who submit fingerprints to NGI and whose biographic information is subsequently sent to NCIC receive a Privacy Act statement on the fingerprint card informing them that

their information will be shared with law enforcement agencies, criminal justice agencies, and other agencies responsible for national security or public safety.

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.

Criminal justice agencies generally collect information submitted to the NCIC in connection with law enforcement investigations; consequently, individuals generally do not have the opportunity to object to the collection of this information by the source agencies or to the sharing and retention of the information in the NCIC. Likewise, individuals generally do not have the opportunity to consent to particular uses of the information in the NCIC since it is obtained incident to criminal justice processes. Individuals in the Identity Theft file consent to the inclusion of their information in the NCIC. Individuals in continuous evaluation tables consent to the use of their information for background check purposes.

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 NCIC. NCIC 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.

Submitting agencies are responsible for the accuracy, timeliness, and relevance of the records they submit to the NCIC. Individuals may work with record owning agencies to correct any inaccuracies with information submitted to the NCIC.

The FBI has published Privacy Act exemptions for access and amendment rights for information in the NCIC. However, individuals may request access to their records by following the guidance provided on the FBI's website at https://www.fbi.gov/services/records-management/foipa. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records. A determination of whether a record may be accessed will be made after a request is received.

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):** 09/17/2019. The NCIC ATO expires on 01/24/2023. The NCIC is currently in the process of being recertified. **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 NCIC 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:** Security controls for the NCIC have been identified by the FBI's Office of the Chief Information Officer and included in the NCIC Security Requirements Traceability Matrix (SRTM). Security controls from the NCIC SRTM have been applied to establish an acceptable security posture that has been authorized by the FBI Authorizing Official.
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:** NCIC audit records are regularly reviewed, and alerts are auto-generated from the CJIS enterprise audit log solution for inappropriate or unusual activity affecting PII. If identified, such activity is investigated and reported, and responsive actions and appropriate mitigations are applied in accordance with FBI incident response plans. Access to NCIC audit records is restricted to FBI system administrators. NCIC network boundaries are automatically and regularly monitored for unusual or suspicious events as part of the CJIS Shared Enterprise Network (SEN) infrastructure by the CJIS Security Operations Center (SOC) and FBI Enterprise Security Operations Center (ESOC).
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:** CSAs must adhere to the following additional training requirements: 1. Within 6 months of employment or assignment, functionally test, and affirm the proficiency of terminal (equipment) operators in order to assure compliance with FBI CJIS policy and regulations. 2. Biennially, provide functional retesting and reaffirm the proficiency of terminal (equipment) operators in order to assure compliance with FBI CJIS policy. 3. Maintain records of all training, testing, and proficiency affirmation. 4. Initially (within 12 months of employment or assignment) provide all sworn law enforcement personnel with basic training in NCIC matters to ensure effective use of the System and compliance with FBI CJIS policy regulation. 5. Make available appropriate training on NCIC System use for criminal justice practitioners other than sworn personnel. 6. Provide all sworn law enforcement personnel and other practitioners with continuing access to information concerning NCIC/state Systems using methods such as roll call and in-service training. 7. Provide peer-level training on NCIC System use, regulations, policy, audits, sanctions, and related civil liability for criminal justice administrators and upper-level managers. 8. Annually review all curricula for relevancy and effectiveness.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The inclusion in the NCIC of information regarding individuals creates a risk that information regarding the individuals may be accessed or disclosed without authorization. To mitigate the risk of unauthorized access and disclosure, NCIC policies include strict dissemination and security requirements to ensure that only authorized users are accessing or receiving NCIC information, and that the information is being used only for authorized purposes. As explained in Section 4 above, access to the NCIC is controlled by ORI. Each agency authorized to access NCIC is assigned an ORI. To receive an ORI, an agency must demonstrate that it meets the legal requirements in 28 CFR Part 20 for access to the NCIC or provide other federal authority for its receipt of NCIC information. Once assigned an ORI, the ORI type determines which information in NCIC an agency can access.

The CSA is responsible for establishing and administering an IT security program throughout the CSA's user community. The CSA must set, maintain, and enforce the following: standards for the selection, supervision, and separation of personnel who have CJIS systems access; policy governing

the operation of hardware and software, and other components used to process, store, or transmit NCIC information to ensure the priority, integrity, and availability of service; security controls governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit FBI data; and standards that provide for audits, the discipline of *CJIS Security Policy* violators, and the monitoring of networks accessing CJIS systems to detect security incidents. Each CSA must provide a signed CJIS User Agreement to the FBI CJIS Division before participating in CJIS records information programs. The CJIS User Agreement includes the standards and sanctions governing utilization of CJIS systems.

All agencies directly connecting to the NCIC must execute a user agreement. The CJIS User Agreement provides that each agency is responsible for appropriate security measures (as applicable) including the physical security of terminals and telecommunications lines; personnel security, including background screening requirements; technical security to protect against unauthorized use; and data security, dissemination, and logging. In addition, each CSA must ensure that all agencies establish an information security structure that complies with *CJIS Security Policy* requirements. NCIC users must comply with the *CJIS Security Policy*, which establishes standards to ensure the confidentiality, integrity, and availability of system data throughout the NCIC user community. The *CJIS Security Policy* requires state and national fingerprint-based record checks upon initial employment or assignment for all personnel who have authorized access to the system and those who have direct responsibility to configure and maintain computer systems and networks with direct access to the system. User computer sites and related infrastructures must always have adequate physical security to protect against any unauthorized access to or routine viewing of computer devices, access devices, and printed and stored data. Automated logs must be maintained on all systems transactions, and security audits for operational systems must be conducted at least once every three years. Each agency accessing the NCIC must meet training requirements, including compliance with operator training mandates. Federal users searching the NCIC via the NCIC Mobile Service must be certified through their respective Terminal Agency Coordinator to use the NCIC Mobile Service. Each agency is responsible for maintaining the integrity of the system in accordance with the FBI CJIS Division and federal, state, territorial, local, and tribal policies to ensure that terminal access is authorized, only authorized transactions are submitted, and that proper handling and dissemination of CJIS data is enforced.

The NCIC creates and maintains transaction logs, which are monitored and reviewed to detect any possible misuse of system data. System administrators review transaction logs for anomalies and report suspicious activity to the System Security Administrator and the Information System Security Officer. In addition, the CAU conducts a triennial compliance audit of each CSA and a sample of agencies served by the CSA to ensure compliance with the FBI *CJIS Security Policy* and other CJIS policies. The CAU may also conduct ad hoc audits based on reports of violations. In addition, each CSA is responsible for conducting its own compliance audits of the criminal and noncriminal justice agencies within the CSA's user community. The CAU submits findings of non-compliance to the CJIS Advisory Policy Board for review. NCIC access is subject to termination for egregious violations of policy provisions.

In addition to the NCIC transaction log, NCIC maintains system audit log data (e.g., privileged user logins, privileged user role escalations, failed password attempts). NCIC audit records are regularly reviewed, and alerts are auto-generated from the CJIS enterprise audit log solution for

inappropriate or unusual activity affecting PII. If identified, such activity is investigated and reported, and responsive actions and appropriate mitigations are applied in accordance with FBI incident response plans. Access to NCIC audit records is restricted to FBI system administrators and information technology security team. NCIC network boundaries are automatically and regularly monitored for unusual or suspicious events as part of the CJIS Shared Enterprise Network (SEN) infrastructure by the CJIS Security Operations Center (SOC) and FBI Enterprise Security Operations Center (ESOC). The NCIC System Security Administrator and Information System Security Officer review system audit logs when alerts trigger or at least every seven (7) calendar days.

All FBI employees and contractors with access to NCIC must maintain an active, adjudicated security clearance. All personnel must complete privacy and information security training annually.

All entities to which the FBI provides an extract of NCIC information for purposes other than synchronizing a state system with the NCIC sign a MOU or similar agreement outlining what information will be shared, the purpose for which the information is being shared, how the information may be used, and requirements for handling the NCIC information. The agreements include provisions requiring the handling of PII in accordance with the Privacy Act and other applicable state and federal laws; reporting any inaccuracies in the NCIC data; and reporting any unauthorized use, disclosure, or access to NCIC information. The CAU has the authority to audit any entity that receives NCIC information to ensure the appropriate access, use, and dissemination of NCIC information.

The FBI manages communications between the NCIC and CSA systems. Network boundary protections including firewalls, intrusion detection systems, and proxy devices are deployed between FBI systems and the constituent systems as part of the CJIS SEN. Any CSA system accessing the NCIC via a "public network" segment must meet the approved form of data encryption and authentication.

The NCIC is transitioning to a cloud environment. When transitioned, the NCIC will use Amazon Web Services' (AWS) government cloud (GovCloud) environment as infrastructure-as-a-service. AWS owns the AWS GovCloud environment. Access to FBI information in the cloud infrastructure is limited to FBI personnel. Access by FBI personnel to specific FBI applications and datasets is determined at the application and dataset level. Audit logs and user login identifiers are collected and maintained by both the FBI and AWS; however, AWS personnel do not have the capability to access FBI applications or datasets, or to audit user activity therein. Data in transit is encrypted using Transport Layer Security (TLS) Federal Information Processing Standard (FIPS) 140-2 encryption, and all interconnections between the AWS GovCloud and the FBI utilize firewalls and security filtering. The NCIC will also use FIPS 140-2 compliant encryption at rest for all data in the cloud.

The NCIC has inter-networked connections with the following FBI infrastructure systems which provide information technology (IT) support services to the NCIC: CJIS SEN, CJIS Unclassified Network (CJIS UNet), FBI UNet, and CJIS Enterprise Storage System (ESS).[15]

[15] The listed FBI infrastructure systems have separate privacy documentation, as necessary.

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.)

Records within the NCIC are retained and disposed of in accordance with its National Archives and Records Administration (NARA) approved records retention schedule, Job Number N1-065-11-3. Generally, NCIC records are retained in an active status until their expiration date is reached or they are cleared or canceled by the entering agency. Records in the following files do not have an expiration date: Wanted Person File, Foreign Fugitive File, Missing Person File, Protective Interest File, TSC File, Immigration Violator File, Unidentified Person File, Violent Person File, NDTF, and Gun File. In addition, the contributing agencies may designate records in the following files as non-expiring: Supervised Release File, Protection Order File, ERPO File, the NSOR, and the Gang File.

Inactive records in the NCIC are removed from active status prior to their expiration date upon being cleared by the contributing agency. Upon removal from active status, NCIC records may be retained online in inactive status for general reference until retired. Inactive sex offender records will be available online for the life of the NCIC system. Inactive protection order records are available online for five years.

Retired records will be deleted/destroyed when 110 years old or when no longer needed for investigative purposes, whichever is later. Retired records are not directly accessible by most NCIC users, but, in most cases, continue to be available for investigative purposes to FBI personnel and CSAs.

The Transaction Log will be maintained until NCIC is discontinued. The Transaction Log now maintains the transaction history for the life of the system; however, the transaction history prior to 1990 was maintained for 10 years.

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.

Information in NCIC qualifies as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, but the system has been excepted from many of the provisions of the Privacy Act because of the underlying criminal justice purposes associated with the maintenance of the database.

NCIC users routinely search the NCIC via text-based queries using primarily biographic descriptors (e.g., name, date of birth, gender, driver's license number, agency number). Specific retrieval parameters for each NCIC file category are described below;

however, authorized FBI personnel and CSAs have enhanced search capabilities which are not limited to specific retrieval parameters.

Information is retrieved from the **Vehicle, License Plate, Boat, Gun, Article, Securities, Vehicle/Boat Part, and Image** files with identifying numbers, such as the vehicle identification number, license plate number, serial number, and NIC number. In addition, information is routinely retrieved from the Securities file with the name and Social Security number of the security's owner.

The person files within the NCIC are retrieved using the following criteria:

Records in the **Wanted Person and Foreign Fugitive Files** are routinely retrieved by a name and one or more of the following numerical identifiers: date of birth, FBI Number/UCN, Social Security number, driver's license number, MNU, or originating agency case number; by a vehicle identification number or license plate number known to be in the possession of an individual in the files; or by a NIC number. A query of the Wanted Person File will also search the Foreign Fugitive, Gang, Identity Theft, Immigration Violator, TSC, NSOR, Protection Order, ERPO, Supervised Release, Protective Interest, and the Violent Persons Files. Inquiries containing vehicle identifiers will also search the License Plate, Vehicle/Boat Part, and Vehicle Files. Inquiries that contain an MNU, Social Security number, or operator's license number will also search the Article File.

Records in the **NSOR File** are retrieved with the same criteria as the Wanted Person file but can also be retrieved by an Internet identifier such as an email address or username. Users can also conduct a direct inquiry into the NSOR File with a zip code.

Records in the **Protective Interest, Gang, TSC, Supervised Release, Case Subject List, Immigration Violator, NICS Denied Transaction, and Violent Person Files** are retrieved using the same criteria as the Wanted Person File. Information in the Gang file can also be retrieved by gang code, city, or state.

Records in the **Missing Person File** are retrieved by the same criteria as the Wanted Person File. The records in the Missing Person File may also be retrieved by the biographic descriptors of the missing person (age, sex, race, height, weight, eye color, and hair color); and by name and date of birth or Social Security number of a person with information about the missing person, if listed in the missing person record.

Records in the **Protection Order File** are retrieved using the same criteria as the Wanted Person File. In addition, records in the Protection Order File can be retrieved by the protected person's name and one of the following: date of birth, Social Security number, or protection order number.

Records in the **Extreme Risk Protection Order (ERPO) File** are retrieved using the same criteria as the Wanted Person File. In addition, NCIC users can retrieve records in the ERPO File by the NCIC number assigned to the ERPO record.

Records in the **Unidentified Person File** are retrieved by including all of the following descriptors: age, sex, race, height, weight, eye color, and hair color; or by NIC number.

Records in the **Identity Theft File** are retrieved by the same criteria as the Wanted Person File except the records cannot be retrieved by vehicle identification number, or license plate number.

Images within the NCIC can be retrieved from the **Image File** by NIC number or image number included in the associated NCIC record. Images of generic vehicles can be retrieved with the vehicle make, vehicle model, vehicle style, and vehicle year. Images of generic boats can be retrieved with the boat make, boat model, boat style, and boat year.

Records in the **ORI File** can be retrieved by full or partial ORI number.

Inactive Records have the same retrievability parameters as the active records. ATF Violent Felon, Retired Records, certain Investigative Subjects of Interest records, and Transaction Log Files are retrievable only by FBI staff and CSAs through enhanced search capabilities.

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 Crime Information Center (NCIC), JUSTICE/FBI-001, 84 Fed. Reg. 47533 (Sep. 10, 2019), available at: https://www.govinfo.gov/content/pkg/FR-2019-09-10/pdf/2019-19449.pdf

Section 8: Privacy Risks and Mitigation

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

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.***

The NCIC maintains criminal justice information about individuals provided by criminal justice agencies for criminal justice (and authorized noncriminal justice) purposes. Through the CJIS Advisory Policy Board, the FBI works with the criminal justice community to determine the scope of information necessary for inclusion in the NCIC to meet criminal justice needs. Generally, the information is not obtained directly from the individual to whom it pertains and therefore there is a risk that the NCIC may contain inaccurate or incomplete information. To mitigate this risk, agencies entering records in the NCIC are responsible for their accuracy, timeliness, and completeness. NCIC policy includes strict validation requirements ensuring that criminal justice agencies periodically

review their records to ensure that they are accurate, timely, relevant, and complete. If agencies do not timely validate a record, the record is purged from the active NCIC file and retired. Once a record is entered into NCIC, only the entering agency can alter or change the record.[16] In addition, NCIC policy includes hit confirmation requirements ensuring that before any user takes action based on active records in the NCIC, the user confirms the validity and accuracy of the record with the agency that submitted the record to the NCIC. The FBI, as manager of the NCIC System, also maintains the integrity of the system through: automatic computer edits which reject record submissions that contain certain common types of errors; automatic purging of records after they meet the expiration date; quality control checks by FBI CJIS Data Integrity staff; and periodically furnishing lists of active records on file for validation by the entering agencies.

Inclusion of individuals' information in the NCIC also creates a risk that the individuals might be subject to increased law enforcement scrutiny. The FBI mitigates the risk of unwarranted law enforcement scrutiny through policy setting forth strict entry criteria for each file and requiring documented interactions with a criminal justice agency to establish compliance with entry criteria. Where necessary, the NCIC includes caveats with disseminated records informing authorized users about the limited purposes for which the information may be used. Moreover, compliance with the NCIC validation requirements helps to ensure that information about individuals will not remain in active NCIC files if criminal justice agencies no longer have an interest in the individual or if the records are no longer actionable. Before any user can take action on active records within the NCIC, NCIC policy requires the user to confirm the validity and accuracy of the record with the agency that submitted the record to the NCIC. These policy requirements ensure that NCIC users receive information only about individuals when there is a legitimate criminal justice interest in the individual.

NCIC also contains information about individuals voluntarily provided to agencies for noncriminal justice purposes (e.g., individuals subject to continuous evaluation or ongoing suitability determinations, searches of biographical information from fingerprint submissions to NGI for licensing and employment). Individuals voluntarily provide this information to record entering agencies; consequently, the information is more likely accurate and complete. Agencies collect this information to provide individuals with government benefits or to conduct employment background checks. Therefore, it is in the individuals' interests to ensure they provide accurate and complete information. The NCIC restricts access to information in the continuous vetting tables to the agencies which enter the information, which mitigates the individuals' risk of increased law enforcement scrutiny from inclusion in the NCIC. Individuals who are only queried through the NCIC are only captured in the transaction log. Information from the transaction log is only provided to criminal justice agencies upon request when the criminal justice agency has a need to know the information for audit, misuse, or active criminal justice investigations.

As discussed above, active records in NCIC are subject to validation requirements, expiration timeframes, and confirmation requirements. Retired records remain in NCIC, but they are only disseminated though offline searches performed by the FBI and CSAs. The dissemination of retired records creates a risk that NCIC users may receive stale or inaccurate information about individuals.

---

[16] The FBI creates all records in the ORI file; however, both the FBI and the agency assigned the ORI can update the agency information in the ORI file.

This risk is mitigated because retired records returned via offline searches include an indicator regarding the record's status (e.g., expired, cleared). Access to the NCIC transaction log is currently limited to authorized FBI personnel. FBI staff can search the Transaction Log for validation, audit, misuse, and criminal justice purposes. Criminal justice agencies may request a search of the transaction log for active investigations; however, information provided from the transaction log is only provided as an investigative lead.