Federal Bureau of Investigation

Privacy Impact Assessment
for the
National Crime Information Center (NCIC)

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

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

Date approved: [March 12, 2019]

(May 2015 DOJ PIA Form/FBI revision August 1, 2017)

EXECUTIVE SUMMARY

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 selected 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.> This Privacy Impact Assessment is being completed to provide an overview of the types of personally identifiable information contained in the NCIC and the use of the information to further criminal justice objectives.

Section 1: Description of the Information System

(a) The Purpose of the NCIC

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.

(b) How the NCIC Achieves its Purpose

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 authorized users enter records into the NCIC, which, in turn, are accessible to authorized agencies nationwide and selected foreign agencies. The NCIC queries allow authorized agencies to quickly and efficiently receive criminal justice information on individuals they encounter while performing their criminal justice and national security missions.

(c) Information in the NCIC

The NCIC contains a variety of law enforcement sensitive files and 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 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. This information is further explained below in subparagraph d, *Access to the NCIC*.

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 records: 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.

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

[1] The FBI Number/UCN is a unique identification number assigned to each fingerprint submission to 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.

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 update records in this File to indicate it has an interest in a wanted person. 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 noted above. 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 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 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.

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 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 serves to warn law enforcement officers of the potential danger posed by individuals and to promote 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 the purpose of this file, 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 criminal justice agencies can enter records into the Gang File. Only criminal justice agencies can receive information from the Gang File.

Known or Suspected Terrorist (KST) File

The KST 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, including individuals, organizations, groups, or networks assessed to be a threat to the safety, security, or national interests of the United States including cyber threat actors, foreign intelligence threat actors, military threat actors, transnational criminal actors, and weapons proliferators as defined in National Security Presidential Memorandum 7, issued on October 5, 2017, or any subsequent authority. The KST file can also accept records on military detainees who are individuals officially detained during military operations who pose an actual

or possible threat to national security, but not persons detained as Enemy Prisoners of War. The FBI's Terrorist Screening Center is the only entity that can enter records into this file, which is available to all 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 regarding 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 records into 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.

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, the File contains generic images that can be used as references for particular makes and models of vehicles and boats. All images submitted to the Image File must be associated with a record in another NCIC file. Primarily only 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.

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 criminal justice agencies may enter records into the Unidentified Person File; however, NCMEC can update the records in this File to

indicate it has an interest in an unidentified person. 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 on property. These files may include some personally identifiable information (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 has built. All the NCIC Files include a miscellaneous field that can be filled with any information including additional PII. Generally, all criminal justice agencies can enter records into the property files. All authorized NCIC users have query access to 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. The information kept within this File includes the brand name, model, serial number, and an owner applied number (if applicable) of the property listed. Only 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. The information contained in this File includes the serial number, caliber, make, type, and model of the weapon listed. Only criminal justice agencies can enter records into the Gun 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.

License Plate File

The License Plate File contains records of stolen license plates. The information contained in this 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 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. The information contained in this 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 criminal justice agencies can enter records into the Vehicle 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 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 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 criminal justice agencies can enter records into this file.

Originating Agency Identifier (ORI) File

Agencies must have an ORI in order 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.

3. 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 or 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 these 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

---

[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.

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 of 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.

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 revetting 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. Criminal justice agencies may request a search of the transaction log for active investigations.

The NCIC maintains a non-operational environment (NOE). Users may access the NOE for user training or software development purposes. The NOE does not contain actual NCIC data, only test transactions.

(d) Access to the NCIC

NCIC users access the NCIC through regional and/or state computer systems or, in some cases, through a direct line to 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 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[6] have access to all information within the NCIC and have the capability to perform "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 within the NCIC.

In general, criminal justice agencies have read and write terminal access to NCIC files, which may include the ability to make additions and changes to the records they have provided to the system. In contrast, noncriminal justice agencies and nongovernmental entities generally will 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, a request is reviewed 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 to which the agency can have access. All ORIs are validated on a biannual basis by the appropriate CSA to confirm all

[6] FBI NCIC program users include CJIS Division personnel in the Investigative and Operations Assistance Group (IOAG), and the NCIC Operations and Policy Unit (NOPU), Global Law Enforcement Support Section.

information associated with each ORI is current and accurate and to confirm the agency is still authorized 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.[7] 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 of criminal justice agencies. Examples of criminal justice agencies include local, state, tribal, federal, and Canadian law enforcement agencies, courts,[8] probation and parole, prosecutors, and correctional facilities.[9] Criminal justice and other authorized agencies with full access ORIs have read and write terminal access to NCIC Files, which includes the ability to enter and make additions and changes to records they have provided in the system. Unless stated otherwise 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. In such cases, the noncriminal justice agency 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

---

[7] The phrase "allocates a substantial part" has been interpreted to mean more than 50 percent of an agency's annual budget.

[8] Courts that hear only civil cases are not considered criminal justice agencies.

[9] Facilities that house only juveniles who are not involved in the criminal justice process but who are orphaned or declared incorrigible are not considered criminal justice agencies.

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 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 set up 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 modify a record to indicate that it has an interest in the 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.

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 and enter/modify access to the Wanted Person, Missing Person, and Protection Order Files.

Authorized governmental agencies, e.g., agencies affiliated with the Department of Children and Family Services, have query access to the Wanted Persons file and may conduct name inquiries of the Interstate Identification Index (III) for the emergency placement of children in limited instances when the primary caretaker is unavailable if the state has a qualifying statute under Pub. Law 92-544.

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

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.

Approved Public Housing Agencies for the Department of Housing and Urban Development have query access to all files in NCIC.

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 CJIS Audit Unit (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. This is accomplished through a review of 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 within their jurisdiction that access NCIC.

CSAs assume responsibility for and enforce system security with regard to 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 and transaction logs 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 Housing of Urban Development receives an extract of the Wanted Person File and an extract of the NSOR file twice a year. 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 that receive an extract of NCIC information that is not used for system synchronization purposes enter into an 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 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.

(e) Retrieval of Information from the NCIC

NCIC users 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 may be 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 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; by address information; or by a NIC number. A query of the Wanted Person File will also search the Foreign Fugitive, Gang, Identity Theft, Immigration Violator, KST, NSOR, Protection Order, 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.

Records in the **Protective Interest, Gang, KST, 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, except they cannot be retrieved using address information. 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 except the records cannot be retrieved by address information. 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, except records cannot be retrieved using address information. Additionally, 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 **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, license plate number, or address information.

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.

(f) Transmission of Information to and from the NCIC

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).[10] 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. 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 matching biographic descriptors 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.

The NCIC data may be directly accessed by authorized NCIC users by means of remote online electronic queries (also known as message keys) submitted to the NCIC via the dedicated telecommunications channels (i.e., the particular query is being made directly to the NCIC). The NCIC data may also be searched by automated referral of queries made to other authorized interoperable systems when the users of the other systems would also be authorized access to the NCIC (i.e., the particular query is being made to another system which passes the query to NCIC). The results of NCIC searches conducted via interoperable systems are sent to authorized users through the interoperable system. For example, an authorized user could search NCIC information from the National Data Exchange and have NCIC search results display within the National Data Exchange. NCIC's connections with other systems are described below. The NCIC data may also be accessed and retrieved locally by authorized DOJ personnel. Such data may be used for authorized DOJ purposes, and/or may be forwarded to other authorized NCIC users for whom direct access is not available. For example, law enforcement agencies may run NCIC queries for, and provide NCIC information to, child support enforcement agencies that are authorized to have access to the NCIC but do not have their own dedicated NCIC terminal.

---

[10] LEEP has separate privacy documentation.

(g) Connections with Other Systems

The NCIC has inter-networked connections with the following FBI infrastructure systems which provide information technology (IT) support services to the NCIC: CJIS Shared Enterprise Network (CJIS SEN), CJIS Unclassified Network (CJIS UNet), FBI UNet, and CJIS Enterprise Storage System (ESS).[11] 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 may conduct named based searches of NGI via the III.

Information within the NCIC can also be retrieved via the NICS, the National Data Exchange System, and the NGI via a secure, internal CJIS network. For example, if a fingerprint based search on an individual is submitted 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 is notified of the match. The NCIC operating manual and code manual are stored on LEEP. LEEP also provides access to multiple NCIC web user interfaces.[12]

(h) Type of System

The NCIC has been categorized as an Information System.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated.

(Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license	X	Financial transaction	
Employee ID		Passport	X	Patient ID	
File/case ID	X	Credit card			

[11] The listed FBI infrastructure systems have separate privacy documentation, as necessary.
[12] NICS, the National Data Exchange System, NGI, and LEEP all have separate privacy documentation.

Other identifying numbers (specify): 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.

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name	X	Place of birth	X	Financial info	
Alias	X	Home address	X	Medical information	X
Gender	X	Telephone number	X	Military service	
Age	X	Email address	X	Physical characteristics	X
Race/ethnicity	X / X	Education		Mother's maiden name	
Other general personal data (specify): 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.					

Work-related data					
Occupation	X	Telephone number	X	Salary	
Job title	X	Email address	X	Work history	
Work address	X	Business associates			
Other work-related data (specify): This information may be contained in the NSOR File, and work related data could be present in the miscellaneous field of any record.					

Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	
Other distinguishing features/biometrics (specify): The NCIC does not include biometrics, other than as listed above; however, the entries may include textual information indicating that subjects' biometrics are available in another system (e.g. fingerprints in NGI; DNA or dental profiles available from a criminal justice agency).					

System admin/audit data					
User ID	X	Date/time of access	X	ID files accessed	X
IP address		Queries run	X	Contents of files	X

System admin/audit data
Other system/audit data (specify): 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 above checked information is captured.

Other information (specify)

2.2 Indicate sources of the information in the system. (Check all that apply.)

Directly from individual about whom the information pertains					
In person		Hard copy: mail/fax		Online	
Telephone		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	X		
Other (specify):					

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.					

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from

sources other than the individual, explain why.)

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 within the NCIC to meet criminal justice needs. The information is not obtained directly from the individual to whom it pertains and therefore there is a risk that inaccurate or incomplete information in the system may be retained unfairly. To mitigate this risk, agencies that enter records into 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 a record is not timely validated, it is purged from the active NCIC file and retired. Additionally, NCIC policy requires that before any user can take action on active records within the NCIC, the user must confirm 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 are in a file for a prescribed period of time; quality control checks by FBI CJIS Data Integrity staff; and periodically furnishing lists of active records on file for validation by the agencies that entered them.

Additionally, there is a risk that inclusion of individuals' information within the NCIC might subject those individuals to increased law enforcement scrutiny. This privacy risk is mitigated, however, because association of an individual with active NCIC files is based on documented interactions with a criminal justice agency and is only permissible if the entry criteria established by policy is met. Where necessary, caveats are added to the dissemination of NCIC information informing authorized users on 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 the individual is no longer of interest to criminal justices agencies or if the records are no longer actionable. As stated above, 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. The limited access to information within the NCIC coupled with the validation requirements and the hit confirmation process will minimize the inconvenience that individuals face when interacting with law enforcement while providing criminal justice agencies with information necessary to achieve their criminal justice missions and to protect law enforcement officers.

NCIC information from individuals obtained not as an interaction with a criminal justice agency (e.g. individuals subject to continuous evaluation or ongoing suitability determinations, searches of biographical information from fingerprint submissions to NGI for licensing and employment) lowers the risk that the information is inaccurate or incomplete. These individuals voluntarily provide their information to the requesting agency to receive a benefit or secure employment. Therefore, it is in the individuals' interests to ensure that their information is accurate and complete. In addition, this information is accessible to fewer NCIC users than information in active NCIC files, 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. As discussed above, direct access to the transaction log is limited to authorized FBI personnel. 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.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities	X	For civil enforcement activities
	For intelligence activities	X	For administrative matters
	To conduct analysis concerning subjects of investigative or other interest	X	To promote information sharing initiatives
	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
	Other (specify):		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

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. 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. The NCIC provides a system to receive and maintain information contributed by participating agencies relating to criminal justice and national security missions. The records maintained within the NCIC assist the FBI, criminal justice agencies, and authorized noncriminal justice agencies in apprehending fugitives, combatting acts of terrorism, solving crimes, 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.

3.3 Indicate the legal authorities, policies, or agreements that authorize

collection of the information in the system. (Check all that apply and include citation/reference.)

	Authority	Citation/Reference
X	Statute	28 U.S.C. §§ 533, 534; 42 U.S.C. § 3771; 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
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 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 (based on applicable NARA disposition schedules) 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, KST File, IVF, Unidentified Person File, VPF, 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, 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.

3.5 Analysis: Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.) [In addition to providing a narrative answer, please consult the ISSO/ISSM for the system's National Institute of Standards and Technology (NIST) 800-122 PII Confidentiality Risk Level, and check the applicable Confidentiality Safeguard Security Controls.]

The inclusion in the NCIC of information regarding individuals creates a risk that information regarding the individuals may be misused or lost. To mitigate this risk, 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 above, transaction-based access to the NCIC is controlled by ORI.

User Agreements are executed with agencies that are connected directly to the CJIS Division maintained systems. These agreements provide 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. Additionally, each CSA must ensure that all agencies establish an information security structure that complies with *CJIS Security Policy* requirements. All authorized recipients are subject to the *CJIS Security Policy* and specific provisions in the User Agreement. They are also responsible for complying with all audit requirements for use of CJIS systems. Each agency is responsible for training requirements, including compliance with operator training mandates. Federal users searching the NCIC via LEEP web interfaces complete additional specialized training addressing the limits of searching NCIC via LEEP and appropriate use of NCIC information. 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.

In addition, the CJIS Division Audit Unit conducts triennial audits of all federal, state, and territorial repositories and a representative sample of local agencies to ensure compliance

with policy. Findings of non-compliance are submitted to the CJIS Advisory Policy Board for review. NCIC access is subject to termination for egregious violations of policy provisions.

All FBI employees and contractors with access to NCIC are required to maintain an active, adjudicated security clearance. Also, all personnel are required to undergo annual privacy and information security training.

PII Confidentiality Risk Level:

☐ **Low** ☐ **Moderate** ☑ **High**

- Is the system protected as classified; or
- Does the system involve intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system; or
- Is the system critical to the direct fulfillment of military or intelligence missions (excluding routine business or administrative applications, e.g., finance, logistics, personnel management)?

☐ **Yes** ☑ **No**

If Yes, the system meets the NIST 800-59 definition of a National Security System.

Access controls

X	Access Enforcement: Access to run specific NCIC transactions that may create, modify, or return NCIC record data containing PII is controlled by the NCIC software based on the CSA ORI and NCIC logical line number used for the transaction. User access to NCIC record data is highly restricted by user roles.
X	Separation of Duties: NCIC users are only allowed access to the information that they need to access in order to complete assigned responsibilities. NCIC users are defined to user groups that are based on user roles that limits the user's access levels. NCIC systems permissions are configured to limit user access. User access to NCIC record data is highly restricted by user roles.
	Least Privilege: Access to run specific NCIC transactions which allows access to NCIC record data containing PII is controlled by the NCIC software based on the CSA ORI and NCIC logical line number used for the transaction. FBI user access to NCIC record data is highly restricted by user roles.
X	Remote Access: No direct Internet-based remote access is permitted to NCIC, and remote access by system administrators is also not permitted. Remote general user access to NCIC is restricted to CSAs and authorized FBI personnel via encrypted connections provided by the CJIS SEN Wide Area Network and virtual private network connections (for CSA disaster recovery sites only) as well as the LEEP.
	User-Based Collaboration and Information Sharing: Not applicable; NCIC does not include capabilities for user collaboration and traditional information sharing. Sharing of

	CSA data is limited to transactional based searches and search results of entered record data.
	Access Control for Mobile Devices: Not applicable; NCIC does not include any mobile devices.
NCIC privileged users are limited to authorized, cleared FBI personnel and contractors. Privileged user access to NCIC is only permitted from internal FBI networks. Authorized federal users have been granted access to some NCIC services from mobile devices; however, these mobile devices are not part of the NCIC information system.	

Audit controls

X	Auditable Events: NCIC audits all transactions and access to the NCIC database containing NCIC records.
X	Audit Review, Analysis, and Reporting: NCIC audit records are regularly reviewed 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.

Identification and Authentication controls

X	Identification and Authentication: NCIC transaction users are the primary users of the NCIC system. In accordance with the *CJIS Security Policy*, CSA users granted NCIC access must authenticate locally to CSA systems prior to establishing connections with NCIC. NCIC then identifies the CSA by the ORI included in each transaction.
NCIC is accessed by CSAs via secured, dedicated network connections provided by the CJIS SEN, and NCIC also restricts access by network addresses. Access to NCIC environments by non-transaction users is restricted to authorized, cleared FBI personnel and contractors.	

Media controls

	Media Access: Not applicable. NCIC does not include nor provide media for offsite transport or use.
X	Media Marking: NCIC system media within FBI facilities are manually marked with a SF710 "UNCLASSIFIED" sticker as needed.
X	Media Storage: NCIC does not include nor provide media for offsite transport or use. NCIC media is limited to media stored and secured within the FBI Data Centers.
	Media Transport: Not applicable; NCIC does not include nor provide media for offsite transport or use.
X	Media Sanitation: All data is unclassified. Sanitization and destruction of physical media is coordinated with and conducted by the FBI Data Centers in accordance with FBI and FBI Data Center's sanitization policy and procedures. NCIC inherits these processes to ensure system components and media are properly sanitized and disposed prior to departing FBI facilities.
NCIC does not include nor provide media for offsite transport or use. Any removable media	

used for storage or transport of NCIC data is managed and controlled separately from the NCIC system following FBI policies to ensure protection of the data.

Data Confidentiality controls

X	Transmission Confidentiality: NCIC general user interfaces including the primary external-facing interfaces used by CSAs for NCIC transactions and reports download are protected via encryption employed by the CJIS SEN and the LEEP.
X	Protection of Information at Rest: NCIC systems are installed in and operate within secured FBI facilities that protect the physical access to the NCIC data stored at rest. IT security alerts are triggered and reviewed anytime information at rest is improperly accessed.

Information System Monitoring

X	Information System Monitoring: NCIC network boundaries are automatically and regularly monitored for unusual or suspicious events as part of the CJIS SEN infrastructure by the CJIS Security Operations Center (SOC), FBI Enterprise SOC (ESOC), and the NCIC security team.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component			X	
DOJ components			X	
Federal entities			X	
State, local, tribal gov't entities			X	
Public				
Private sector	X			
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):				

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.) [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

As discussed in Section 1 above, different NCIC users have access to different information within the NCIC. NCIC data is made available to different users in different ways, depending on the nature of the user and the nature of the data. In general, criminal justice agencies have query and enter/modify access to NCIC files, which may include the ability to make additions and changes to their own records in the system. In contrast, noncriminal justice agencies and nongovernmental entities generally will have query-only access to selected portions of NCIC. Access to the records in the NCIC is controlled by user type and ORI.

User Agreements are executed with agencies that are connected directly to the CJIS Division maintained systems. These agreements provide 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. Additionally, each CSA must ensure that all agencies establish an information security structure that complies with *CJIS Security Policy* requirements. All authorized recipients are subject to the *CJIS Security Policy*, and specific provisions in the User Agreement. They are also responsible for complying with all audit requirements for use of CJIS systems. Each agency is responsible for training requirements, including compliance with operator training mandates. 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.

In addition, the CJIS Division Audit Unit conducts triennial audits of all federal, state, and territorial repositories and a representative sample of local agencies to ensure compliance with policy. Findings of non-compliance are submitted to the CJIS Advisory Policy Board for review. NCIC access is subject to termination for egregious violations of policy provisions.

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 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, 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 on individuals. 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 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.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Because the information is collected in connection with criminal justice interactions and investigations, 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.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how:
X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Because the information is collected in connection with criminal justice interactions and investigations, 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.

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

The agencies that contribute the 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) will provide 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 has developed a consent form available for agencies to use when collecting information for inclusion in the identity theft file informing 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.

Because the information in the NCIC is collected in connection with law enforcement investigations, 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.

When federal agencies provide information about individuals to the NCIC for benefits, employment, and security clearances, and that information is maintained in the NCIC for continuous evaluation or ongoing suitability determinations, those federal agencies 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. 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.

Section 6: Information Security

6.1 Indicate all that apply.

X	A security risk assessment has been conducted.
X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Security controls for the NCIC have been identified by FBI Security Division and included in the NCIC Security Requirements Traceability Matrix (SRTM). Security controls from the NCIC SRTM have been applied in order to establish an acceptable security posture that has been authorized by the FBI Authorizing Official.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: NCIC audit records are regularly reviewed 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. NCIC network boundaries are automatically and regularly monitored for unusual or suspicious events as part of the CJIS SEN infrastructure by the CJIS SOC, FBI ESOC, and the NCIC security team. The CJIS Audit Unit also performs reviews of CSAs granted NCIC access to ensure proper use of the NCIC.
X	The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Certification and Accreditation: 03/31/2016. The NCIC is currently in the process of being recertified.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: NCIC audit records are regularly reviewed 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 SEN infrastructure by the CJIS SOC and FBI ESOC.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.

X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.		
X	The following training is required for authorized users to access or receive information in the system:		
	X		General information security training
	X		Training specific to the system for authorized users within the Department.
	X		Training specific to the system for authorized users outside of the component.
			Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure. [In answering the question, you should discuss the relevant NIST Confidentiality Safeguard Security Controls.]

NCIC data is security authorized pursuant to the FISMA following requirements and standards from the OMB Circular A-130, and the NIST Special Publications 800-37 and 800-53 requirements. The system's technical security design supports and secures IT functionality in accordance with federal guidelines and commercial best practices.

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

NCIC users are required to 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 have adequate physical security at all times 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.

The CSA is responsible for establishing and administering an IT security program throughout the CSA's user community. The CSA is responsible to 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 written agreement to the FBI CJIS Division before participating in CJIS records information programs. This agreement includes the standards and sanctions governing utilization of CJIS systems.

Each agency is assigned an ORI to access the NCIC. The system creates and maintains transaction logs, which are monitored and reviewed to detect any possible misuse of system data. The FBI CJIS Audit Unit 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 FBI CJIS Audit Unit 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.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: *National Crime Information Center (NCIC)*, JUSTICE/FBI-001, 84 Fed. Reg. 47533 (Sep. 10, 2019)
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information in the NCIC is retrieved by name or other identifiers. Certain NCIC users may retrieve information from the NCIC using any data field within the NCIC. For more detailed information on the retrieval parameters for the specific NCIC files, please see the *"Retrieval of Information from the NCIC"* portion of section 1 on the instant PIA.