Billing Code 4410-02-P

DEPARTMENT OF JUSTICE

[CPCLO Order No. 006-2019]

Privacy Act of 1974; System of Records

AGENCY: Federal Bureau of Investigation, United States Department of Justice.

ACTION: Notice of a Modified System of Records.

SUMMARY: Pursuant to the Privacy Act of 1974, and Office of Management and Budget (OMB) Circular No. A-108, notice is hereby given that the United States Department of Justice (Department or DOJ), Federal Bureau of Investigation (FBI), proposes to modify a system of records entitled National Crime Information Center (NCIC), JUSTICE/FBI-001, which was last published in the **Federal Register** on September 28, 1999 (64 FR 52343). The NCIC serves as a central information repository to assist criminal justice professionals in apprehending fugitives, locating missing persons, recovering stolen property, and identifying known or suspected terrorists. Law enforcement officers also use the information within NCIC to help protect the general public and themselves when carrying out their official duties. This system of records notice is being updated to better inform the public about the types of information within the NCIC and the uses of this information to further criminal justice purposes.

DATES: In accordance with 5 U.S.C. 552a(e)(4) and (11), this system of records begins on publication, subject to a 30-day period to comment on the routine use modifications described below. Please submit any comments by [INSERT DATE 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: The public, OMB, and Congress are invited to submit any comments: by mail to the Department of Justice, Office of Privacy and Civil Liberties, ATTN: Privacy Analyst, 145 N

St., NE, Suite 8w-300, Washington, D.C. 20530; by facsimile at 202-307-0693; or by email at *privacy.compliance@usdoj.gov*. To ensure proper handling, please reference the above CPCLO Order No. on your correspondence.

FOR FURTHER INFORMATION CONTACT: Katherine M. Bond, Assistant General Counsel, Privacy and Civil Liberties Unit, Office of the General Counsel, FBI, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001; telephone (202) 324-3000.

SUPPLEMENTARY INFORMATION: The FBI has revised this system of records notice to update information about this system. Established in 1967, the NCIC is a national criminal justice information system linking criminal (and authorized non-criminal) justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, as well as selected foreign countries to facilitate the cooperative sharing of criminal justice information. *See* 28 C.F.R. Sections 20.3(b) & (g) for definitions of "administration of criminal justice" and "criminal justice agency." The NCIC provides a system to receive and maintain information contributed by participating agencies relating to criminal justice and national security missions. 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). The purposes of maintaining records in the NCIC include combatting acts of terrorism; apprehending fugitives; 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 firearms, licensee, and explosive background checks; and enhancing the safety of law enforcement officers.

This Notice modifies the previous publication of the NCIC System of Records Notice to (1) include new categories of records and individuals, (2) update routine uses, and (3) remove

references to the Interstate Identification Index (III). Since the September 28, 1999, publication of notice of this System of Records, 64 FR 52343, criminal justice agencies have requested that additional information be included in the NCIC to meet their needs.. This additional information includes such new categories of individuals and categories of records as the National Sex Offender Registry, the Supervised Release File, the Identity Theft File, the Protective Interest File, the NICS Denied Transaction File, the Immigration Violator File, and the Violent Person File. Adding this information to the NCIC advances FBI's mission and criminal justice investigation, as well as increasing officer safety by providing pertinent information to law enforcement officers regarding the individuals they encounter while on duty.

This System of Records Notice also updates the routine uses for the information contained within the NCIC to educate the public on how the records will be shared with criminal justice agencies, authorized non-criminal justice agencies, and private organizations to further the purposes of combatting acts of terrorism; apprehending fugitives; 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 firearms, licensee, and explosive background checks; and enhancing the safety of law enforcement officers. For consolidation and transparency purposes, the routine uses applicable to the NCIC under the FBI's Blanket Routine Uses (**FBI-BRU,** 66 FR 33558 (June 22, 2001), as amended by 70 FR 7513, 517 (Feb. 14, 2005) and 82 FR 24147 (May 25, 2017)) are also being included in the routine use portion of this notice.

Finally, this modified System of Record Notice removes references to the Interstate Identification Index (III) and criminal history record information. Although the NCIC is used to retrieve criminal history record information from III through a federated search capability, III is

not part of NCIC, and criminal history record information is no longer maintained within the NCIC, but is now maintained in the FBI's Next Generation Identification (NGI) System, JUSTICE/FBI-009, 81 Fed. Reg. 27284 (May 5, 2016). A person who wishes to access his or her criminal history records should follow the procedures set forth in 28 C.F.R. § 16.30 *et seq.*

In accordance with 5 U.S.C. 552a(r), the Department has provided a report to OMB and the Congress on this revised system of records notice.

Dated: August 28, 2019.

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer,
United States Department of Justice.

SYSTEM NAME AND NUMBER:

National Crime Information Center (NCIC), JUSTICE/FBI-001.

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Records may be maintained at all locations at which the FBI operates or at which FBI operations are supported, including: J. Edgar Hoover Building, 935 Pennsylvania Avenue, NW, Washington, DC 20535-0001; FBI Academy and FBI Laboratory, Quantico, VA 22135; FBI Criminal Justice Information Services (CJIS) Division, 1000 Custer Hollow Road, Clarksburg, WV 26306; FBI Records Management Division, 170 Marcel Drive, Winchester, VA 22602-4843; and FBI field offices, legal attaches, information technology centers, and other components listed on the FBI's Internet Web site, *https://www.fbi.gov*. Some or all system information may also be duplicated at other locations where the FBI has granted direct access for support of FBI missions, for purposes of system backup, emergency preparedness, and/or continuity of operations.

SYSTEM MANAGER(S):

Director, Federal Bureau of Investigation, 935 Pennsylvania Avenue, NW Washington, DC 20535-0001; (202) 324-3000.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Authorities for maintaining the system include 28 U.S.C. Chapter 33; and 28 CFR 0.85 and 28 CFR Part 20. Additional authorities include 34 U.S.C. Chapter 10211; the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, 115 Stat 272; the Intelligence Reform

and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. 108-458, 118 Stat 3638; the Implementing Regulations of the 9/11 Commission Act of 2007, Pub. L. 110-53, 121 Stat 266; Executive Order 13311, *Homeland Security Information Sharing* (July 29, 2003); Executive Order 13356, *Strengthening the Sharing of Terrorism Information To Protect Americans* (August 27, 2004); and Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information To Protect Americans* (October 25, 2005).

PURPOSE(S) OF THE SYSTEM:

Established in 1967, the NCIC is a national criminal justice information system linking criminal (and authorized non-criminal) justice agencies located in the 50 states, the District of Columbia, U.S. territories and possessions, as well as selected foreign countries, to facilitate the cooperative sharing of criminal justice information. The NCIC provides a system to receive and maintain information contributed by participating agencies relating to criminal justice and national security missions. 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). The purposes of maintaining records in the NCIC include combatting acts of terrorism; apprehending fugitives; 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 firearms, licensee, and explosive background checks through the National Instant Criminal Background Check System (NICS); and enhancing the safety of law enforcement officers.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Categories of individuals covered by the system are:

A. Wanted persons:

1. Individuals for whom federal warrants are outstanding.
2. Individuals who allegedly have committed or have been linked with an offense which is classified as a felony, misdemeanor, or other criminal offense under the existing penal statutes of the jurisdiction originating the entry and for whom a warrant has been issued with respect to the offense that was the basis of the entry; and probation and parole violators meeting these criteria.
3. Individuals for whom a "Temporary Felony Want" has been entered. Temporary felony want records allow a law enforcement agency to take prompt action to apprehend a person suspected of committing a felony when circumstances prevent the agency from immediately obtaining a warrant. Procedural safeguards for these Temporary Felony Wants include that they may only be entered in NCIC for the apprehension of a person who has committed, or the officer has reasonable grounds to believe has committed, a felony; the person may seek refuge by fleeing across jurisdictional boundaries; and (as noted) circumstances preclude the immediate procurement of an arrest warrant. A Temporary Felony Want shall be specifically identified as such and automatically expires 48 hours after entry.
4. Juveniles who (a) have been adjudicated delinquent and who have escaped or absconded from custody, even though no arrest warrants were issued; or (b) who have been charged with the commission of a delinquent act that would be a crime if committed by an adult, and who may have fled from the state where the act was committed.
5. Individuals who allegedly have committed or have been linked with an offense committed in a foreign country that would be a felony if committed in the United

States, and for whom a warrant of arrest is outstanding, and (a) for which act an extradition treaty exists between the United States and that country, (b) are wanted by foreign authorities for a violent crime, or (c) are otherwise known or reasonably believed by foreign authorities to be violent, armed, or dangerous.

6. Individuals who allegedly have committed or have been linked with an offense committed in Canada and for whom a Canada-Wide Warrant has been issued which meets the requirements of the Canada-United States Extradition Treaty.

B. Sex offender registrants: Individuals who are required to register in a jurisdiction's sex offender registry.

C. Violent felons: Individuals with three or more convictions for a violent felony or serious drug offense as defined by 18 U.S.C. 924(e), and who were entered into the NCIC Violent Felon file between 1992 and 1998.

D. Individuals on probation, parole, supervised release, pretrial supervision, or released on their own recognizance; and supervising officials for these individuals.

E. Immigration violators: Criminal aliens who have been previously deported; aliens with outstanding administrative warrants of removal from the United States; aliens who have failed to comply with national security registration requirements; and other immigration violators.

F. Missing persons: Individuals of any age who are missing and for whom there is a reasonable concern for the well-being of the person and/or others, such as: a missing person who suffers from a documented physical/mental disability; a person missing under circumstances indicating that the disappearance was not voluntary or that the person's health or physical safety may be in danger; a missing child under the age of 21 reported

to law enforcement; a person missing after a catastrophe; and, persons reasonably believed to have information regarding missing persons.

G. Persons of protective interest: Individuals designated by local, state, tribal, territorial, and federal law enforcement agencies with a protective mission as presenting credible threats to authorized protectees of those agencies.

H. Members of criminal gangs: Individuals about whom law enforcement agencies have developed sufficient information to establish membership or other similar relationship in a particular criminal gang by either self-admission or pursuant to documented criteria approved by the FBI. 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 or delinquent conduct.

I. Known or suspected terrorists: Individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to domestic or international terrorism.

J. Military Detainees: Individuals who were officially detained during military operations who pose an actual or possible threat to national security, but not persons detained as Enemy Prisoners of War.

K. National Security Threat Actors: 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.

L. Unidentified persons: Any unidentified deceased person or body parts, or any living

person whose identity has not been ascertained (e.g., infant, amnesia victim, catastrophe victim).

M. Persons related to protection orders: Individuals against whom a protection order has been issued and the protected persons.

N. Owners of stolen property related to NCIC entries.

O. Victims of identity theft.

P. 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 National Instant Criminal Background Check System (NICS).

Q. Violent persons: Individuals who have been convicted of violent crimes, or have made credible threats, against law enforcement and individuals who have been convicted of certain other violent crimes.

R. Individuals associated with active FBI investigations such as suspects, subjects of interest, witnesses, or victims.

S. FBI employees, U.S. government employees, and employees of local, state, tribal, or territorial law enforcement agencies.

T. Individuals who are, or within the last five years were, under FBI investigation for terrorism.

U. Individuals named in documents supporting NCIC entries (e.g. warrants, protection orders, terms and conditions of probation/supervised released, missing person reports).

V. Subjects of Continuous Evaluation: Individuals required by statute, executive authority, or other legal authority to undergo continuous revetting to maintain employment or security clearance with a federal agency.

W. 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).

X. Individuals who have been queried through the NCIC. This includes all individuals queried through the NCIC for purposes listed in the "Routine Uses" section of this notice.

CATEGORIES OF RECORDS IN THE SYSTEM:

The NCIC may contain records about individuals described by the categories listed above. Records may include all manner of identifying information, such as name, Social Security number, date of birth, place of birth, physical description, photograph, descriptive information about fingerprints and other biometrics which may be available (the biometrics themselves and not maintained within the NCIC), passport and/or driver's license information, personal and business addresses and telephone numbers, and other personal identifiers. Records in the system may include details pertinent to particular file types, such as law enforcement information, visa/immigration information, and terrorism information; information relevant to the protection of health, safety, or property; physical or medical characteristics or other personal information deemed necessary to identify an individual, protect law enforcement officers, and identify and protect law enforcement subjects; and information relevant to responding to, mitigating, and recovering from disasters, emergencies, and catastrophes, as well as assisting in other humanitarian efforts. Records may also include uploaded documents supporting NCIC entries (e.g. warrants, protection orders, terms and conditions of probation/supervised release, missing person reports). Specific files in the NCIC include:

A. Vehicle File:

    1. Stolen vehicles, including aircraft and trailers.

2. Vehicles wanted in conjunction with crimes.

3. Vehicles subject to seizure based on federal court orders.

B. License Plate File (Stolen).

C. Boat File (Stolen).

D. Vehicle/Boat Part File: Serially-numbered components of vehicles and boats reported to have been stolen.

E. Gun File:

1. Stolen guns.

2. Recovered guns, when ownership has not been established.

3. Lost guns.

4. Guns believed to have been used during the commission of crimes.

F. Article File (Stolen or Lost).

G. Securities File: Serially numbered stolen, embezzled, used for ransom, or counterfeited securities.

H. Wanted Person File: Described in "Categories of Individuals Covered by the System: A (1-4)."

I. Foreign Fugitive File: Described in "Categories of Individuals Covered by the System: A. (5, 6)."

J. National Sex Offender Registry: Described in "Categories of Individuals Covered by the System: B."

K. The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) Violent Felon File: Described in "Categories of Individuals Covered by the System: C." (The ATF no longer enters data into this file, and these records have now been retired and are only accessible

by the FBI.)

L. Supervised Release File: Described in "Categories of Individuals Covered by the System: D."

M. Immigration Violator File: Described in "Categories of Individuals Covered by the System: E."

N. Missing Person File: Described in "Categories of Individuals Covered by the System: F."

O. Protective Interest File: Described in "Categories of individuals Covered by the System: G."

P. Gang File: Described in "Categories of Individuals Covered by the System: H."

Q. Known or Suspected Terrorist File: Described in "Categories of Individuals Covered by the System: I, J, and K."

R. Unidentified Person File: Described in "Categories of Individuals Covered by the System: L."

S. Protection Order File: Described in "Categories of Individuals Covered by the System: M."

T. Identity Theft File: Described in "Categories of Individuals Covered by the System: O."

U. NICS Denied Transaction File: Described in "Categories of Individuals Covered by the System: P."

V. Image File: Identifying images (e.g., mug shots; scars, marks, tattoos; property photos; signatures) and documents to help identify persons and property related to entries in other NCIC files.

W. Violent Person File: Described in "Categories of Individuals Covered by the System: Q."

X. System Tables and Charts: Although not part of particular files described herein, these

tables and charts may contain data elements from the above files (e.g. license plate numbers, vehicle identification numbers); include individuals described in "Categories of Individuals Covered by the System" R, S, T, V, and W; and are used for system administration, investigative, and other authorized purposes.

Y. Inactive Records: Records that are still generally available to all NCIC authorized users for historical reference after the records have expired or been cleared from the active NCIC files.

Z. Retired Records: Records that have expired, been cleared, or been canceled from the active NCIC environment. These records are only directly accessible by FBI personnel and CJIS Systems Agencies.

AA. Transaction Log: All transactions that enter, update, query, or access the records described above; rejected transactions; and system administrative messages. 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. Transaction logs may contain information regarding all "Categories of Individuals." Search criteria from queries initiated by the National Instant Criminal Background Check System (NICS), JUSTICE/FBI-018, are not logged.

RECORD SOURCE CATEGORIES:

Local, state, tribal, territorial, federal, foreign, and international governmental agencies and authorized non-governmental entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES:

These records or information contained therein may be disclosed as routine uses pursuant to 5 U.S.C. 552a(b)(3) of the Privacy Act as described below. As routine uses specific to this system, the DOJ may disclose relevant system records or information to the extent such disclosures are compatible with a purpose for which the information was collected. Routine uses are not meant to be mutually exclusive and may sometimes overlap.

A. To local, state, tribal, territorial, or federal law enforcement or criminal justice agencies (to include police, prosecution, penal, probation, or parole agencies, and the judiciary) or other authorized federal agencies where such disclosure:

1. May assist the recipient in the performance of its law enforcement, criminal justice, or national security functions, to include the screening of employees, contractors, or applicants for employment by criminal justice agencies;

2. May assist the FBI in performing a law enforcement or national security function;

3. May promote, assist, or otherwise serve the mutual efforts of the law enforcement, criminal justice, and national security communities, such as site security screening of visitors to criminal justice facilities and military installations; or

4. May serve a compatible civil law enforcement purpose.

B. To authorized foreign governments or international agencies where such disclosure:

1. May assist the recipient in the performance of its law enforcement, criminal justice, or national functions;

2. May assist the FBI in performing a law enforcement or national security function;

3. May promote, assist, or otherwise serve the mutual efforts of the international community; or

4. May serve a compatible civil law enforcement purpose.

C. To appropriate officials and employees of a federal agency or entity which requires information relevant to a decision concerning the hiring, appointment, or retention of an employee; the issuance, renewal, suspension, or revocation of a security clearance; the execution of a security or suitability investigation; the letting of a contract; or the issuance of a grant.

D. To state and federal agencies when necessary to assist in detecting and preventing fraudulent receipt of government benefits (e.g. Department of Housing and Urban Development, Department of Veterans Affairs, or Social Security Administration).

E. To the Department of State for the purpose of determining the eligibility of visa and passport applicants.

F. To the Department of Homeland Security and its components for use in background investigations of individuals with access to secure areas of airports, aircraft, ports, and vessels; commercial drivers of hazardous materials; applicants for aircraft training; those responsible for screening airport passengers and property; those with security functions related to baggage and cargo; and other statutorily authorized populations.

G. To authorized local, state, tribal, territorial, and federal agencies for the purposes of emergency child placement or emergency disaster response.

H. To authorized non-governmental entities or subunits thereof that perform the administration of criminal justice for criminal justice purposes as defined in 28 C.F.R. § 20.3(b).

I. To authorized local, state, tribal, territorial, federal, foreign, or international agencies for humanitarian purposes (e.g. vetting volunteers during natural disasters).

J. To authorized agencies as required by federal statutes, treaties, executive orders and other presidential and executive directives, federal regulations, federal rules, or Attorney General Guidance.

K. To authorized federal agencies for alien registration, immigration, naturalization, international travel, or similar matters related to national security.

L. To designated points of contact at criminal justice agencies for background checks under the National Instant Criminal Background Check System (NICS).

M. To local, state, tribal, territorial, or federal criminal justice officials for the conduct of firearms or explosives-related background checks when required to issue firearms or explosives-related licenses or permits according to a state statute or local ordinance, when checking firearms transferred to pawn shops, or when returning firearms to authorized recipients.

N. To authorized non-criminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for local, state, tribal, territorial, federal, or foreign criminal justice agencies.

O. To private contractors pursuant to specific agreements with local, state, tribal, territorial, federal, or foreign criminal justice or authorized non-criminal justice agencies for the purpose of providing services for the administration of criminal justice as defined in 28 C.F.R. § 20.3(b).

P. To the National Center for Missing and Exploited Children (NCMEC) when acting

within its statutory duty to support law enforcement agencies.

Q. To local, state, tribal, territorial, and federal government social service agencies with child protection responsibilities for purposes of investigating or responding to reports of child abuse, neglect, or exploitation.

R. To railroad or private college/university police departments or subunits thereof which perform, and allocate a substantial portion of their annual budget to, the administration of criminal justice and whose appropriately trained employees hold police powers under state law for the administration of criminal justice as defined in 28 CFR 20.3(b).

S. To civil or criminal courts for use in domestic violence or stalking cases.

T. To social networking websites to prevent sex offenders from using these websites to entice children. This routine use applies only to disclosing records in the National Sex Offender Registry.

U. To governmental and authorized non-governmental recipients of fingerprint-based background check results from the Next Generation Identification (NGI) System, when information in NCIC records may be relevant to authorized checks of the NGI System (e.g. criminal and non-criminal justice background checks).

V. To the National Insurance Crime Bureau (NICB), a nongovernmental nonprofit agency, for use toward its mission of acting as a national clearinghouse for information on stolen vehicles and offering free assistance to law enforcement agencies concerning automobile thefts, identification, and recovery of stolen vehicles.

W. To authorized private organizations determined to be involved in the administration of criminal justice where the records are necessary and relevant to carry out the administration of a criminal justice function. This routine use is limited to disclosure of

the NCIC property files.

X. To local, state, tribal, territorial, and federal criminal justice agency officials for the purpose of screening visitors to critical infrastructure facilities.

Y. To local, state, tribal, territorial, federal, foreign, or international licensing agencies or associations which require information concerning the suitability or eligibility of an individual for a license or permit.

Z. To such agencies, entities, and persons as the FBI deems appropriate and relevant to ensure the continuity of government functions in the event of any actual or potential disruption of normal government operations. This use encompasses all situations in which government operations may be disrupted, including: military, terrorist, cyber, or other attacks, natural or manmade disasters, and other national or local emergencies; inclement weather and other acts of nature; infrastructure/utility outages; failures, renovations, or maintenance of buildings or building systems; problems arising from planning, testing or other development efforts; and other operational interruptions. This also includes all related prevention activities, pre-event planning, preparation, backup/redundancy, training and exercises, and post-event operations, mitigation, and recovery.

AA. To such agencies, entities, and persons as the DOJ or FBI may consider necessary or appropriate incident to development and testing of FBI information systems and system functionality and integrity, including prototype testing, operational testing, interoperability testing, and vulnerability testing.

BB. To such agencies, entities, and persons as the FBI may consider necessary or

appropriate for research or statistical purposes.

CC. To any agency, entity, or person in either the public or private sector, domestic, foreign, or multinational, if deemed by the FBI to be reasonable and helpful to elicit information or cooperation from the recipient for use by the FBI in the performance of an authorized function.

DD. If any system record, on its face or in conjunction with other information, indicates a violation or potential violation of law (whether civil or criminal), regulation, rule, order, or contract, the pertinent record may be disclosed to the appropriate entity (whether local, state, tribal, territorial, federal, foreign, or international), that is charged with the responsibility of investigating, prosecuting, and/or enforcing such law, regulation, rule, order, or contract.

EE. To contractors, grantees, experts, consultants, students, or others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government, when necessary to accomplish an agency function.

FF. To the news media or members of the general public in furtherance of a legitimate law enforcement or public safety function as determined by the FBI, e.g., to assist in locating fugitives; to provide notifications of arrests; to provide alerts, assessments, or similar information on potential threats to life, health, or property; or to keep the public appropriately informed of other law enforcement or FBI matters or other matters of legitimate public interest where disclosure could not reasonably be expected to constitute an unwarranted invasion of personal privacy. (The availability of information in pending criminal or civil cases will be governed by the provisions of 28 CFR 50.2.)

GG. To a court or adjudicative body, in matters in which any of the following entities is

or could be a party to the litigation, is likely to be affected by the litigation, or has an official interest in the litigation, and disclosure of system records has been determined by the FBI to be arguably relevant to the litigation: (a) the FBI or any FBI employee in his or her official capacity, (b) any FBI employee in his or her individual capacity where the Department of Justice has agreed to represent the employee, or (c) the United States. Similar disclosures may be made in analogous situations related to assistance provided to the Federal Government by non-FBI employees.

HH. To an actual or potential party or his or her attorney for the purpose of negotiating or discussing such matters as settlement of the case or matter, and for formal or informal discovery proceedings, in matters in which the FBI has an official interest and in which the FBI determines records in the system to be arguably relevant.

II. To such recipients and under such circumstances and procedures as are mandated by Federal statute, Executive Order, or treaty.

JJ. To a requesting Member of Congress or a person on his or her staff acting on the Member's behalf when the request is made on behalf of and at the request of the individual who is the subject of the record.

KK. To the National Archives and Records Administration (NARA) for records management inspections and such other purposes conducted under the authority of 44 U.S.C. 2904 and 2906.

LL. To any agency, organization, or individual for the purposes of performing authorized audit or oversight operations of the FBI and meeting related reporting requirements.

MM. The DOJ may disclose relevant and necessary information to a former employee of the Department for purposes of: responding to an official inquiry by a local, state, or

federal government entity or professional licensing authority, in accordance with applicable Department regulations; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information and/or consultation assistance from the former employee regarding a matter within that person's former area of responsibility. (Such disclosures will be effected under procedures established in title 28, Code of Federal Regulations, sections 16.300–301 and DOJ Order 2710.8C, including any future revisions.)

NN. To the White House (the President, Vice President, their staffs, and other entities of the Executive Office of the President (EOP)), and, during Presidential transitions, the President-Elect and Vice-President Elect and their designees for appointment, employment, security, and access purposes compatible with the purposes for which the records were collected by the FBI, *e.g.*, disclosure of information to assist the White House in making a determination whether an individual should be: (1) granted, denied, or permitted to continue in employment on the White House Staff; (2) given a Presidential appointment or Presidential recognition; (3) provided access, or continued access, to classified or sensitive information; or (4) permitted access, or continued access, to personnel or facilities of the White House/EOP complex. System records may be disclosed also to the White House and, during Presidential transitions, to the President Elect and Vice-President Elect and their designees, for Executive Branch coordination of activities which relate to or have an effect upon the carrying out of the constitutional, statutory, or other official or ceremonial duties of the President, President Elect, Vice-President or Vice-President Elect.

OO. To complainants and/or victims to the extent deemed appropriate by the FBI to provide such persons with information and explanations concerning the progress and/or results of the investigations or cases arising from the matters of which they complained and/or of which they were victims.

PP. To designated officers and employees of state, local (including the District of Columbia), or tribal law enforcement or detention agencies in connection with the hiring or continued employment of an employee or contractor, where the employee or contractor would occupy or occupies a position of public trust as a law enforcement officer or detention officer having direct contact with the public or with prisoners or detainees, to the extent that the information is relevant and necessary to the recipient agency's decision.

QQ. To appropriate agencies, entities, and persons when (1) the Department suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, DOJ (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

RR. To another Federal agency or Federal entity, when the Department determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity

(including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Computerized records are stored electronically on hard disk, removable storage devices or other digital media. Some information may be retained in hard copy format and stored in individual file folders and file cabinets with controlled access, and/or other appropriate GSA-approved security containers.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information is retrieved by name or other identifying information. NCIC data may be directly accessed and retrieved by authorized NCIC users by means of remote on-line electronic queries submitted to the NCIC via authorized telecommunications channels. NCIC users are primarily located within the United States, but they also include United States users overseas, as well as foreign users in authorized foreign/international entities. NCIC data may also be retrieved 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. NCIC data may also be accessed and retrieved locally by authorized DOJ personnel. Information accessed locally may be used for authorized DOJ purposes, and/or may be forwarded to other authorized NCIC users for whom direct access is not available. Authorized FBI personnel and CJIS Systems Agencies (agencies which assume responsibility for and enforce system security with regard to all other agencies in a specific state or territory) have enhanced search capabilities and can retrieve all records within the NCIC.

POLICIES AND PROCEDURES FOR RETENTION AND DISPOSAL OF RECORDS:

Records in this system are maintained and disposed of in accordance with appropriate

authority of the National Archives and Records Administration. Generally, records are kept for 110 years or until no longer needed for reference purposes. The NCIC transaction log will be maintained until the system is discontinued.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

A. NCIC records are controlled in accordance with OMB Circular A-130 and National Institute of Standards and Technology 800-37 and 800-53 requirements. Associated FBI information technology (IT) systems are certified and accredited pursuant to the Federal Information Security Modernization Act. The system's technical security design supports and secures IT functionality in accordance with federal guidelines and commercial best practices.

B. The FBI is responsible for managing the communications between the NCIC and constituent user systems. Encryption is used to secure all communications between the NCIC and other FBI systems that are not co-located with the system. Network boundary protections including firewalls, intrusion detection systems, and proxy devices are also deployed between FBI systems and the constituent systems. Any constituent system that is accessing the NCIC via a "public network" segment must meet the approved form of data encryption and authentication. All constituent IT systems with connectivity to the system must employ virus protection software.

C. All FBI employees and contractors who will develop, manage, use, or operate an FBI system receive a computer security awareness briefing prior to being granted any type of FBI system access and are provided with security awareness and privacy training at least annually. All FBI employees receive a complete background investigation prior to being hired and other authorized system support personnel, such as contractors, receive comparable vetting. All FBI

employees and system support personnel are cautioned not to divulge confidential information or any information contained in FBI files. Failure to abide by these provisions violates FBI directives and DOJ regulations and may violate certain civil and criminal statutes.

D. 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 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.

E. A CJIS Systems Agency (CSA) is a duly authorized local, state, tribal, territorial, federal, or foreign criminal justice agency on the CJIS network infrastructure providing state-wide (or equivalent) service to its users. 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, 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.

F. Each agency is assigned an originating agency identifier (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 non-criminal justice agencies within the CSA's user community.

RECORD ACCESS PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a (j) or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the FBI in its sole discretion.

All requests for access should follow the guidance provided on the FBI's website at *https://www.fbi.gov/services/records-management/foipa*. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act

Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 170 Marcel Drive, Winchester, VA 22602-4843; facsimile: 540-868-4995/6/7; electronically: *https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records*. The request should include a general description of the records sought, and must include the requester's full name, current address, and date and place of birth. The request must be signed and dated and either notarized or submitted under penalty of perjury. While no specific form is required, requesters may obtain a form (Form DOJ-361) for use in certification of identity, which can be located at the above link. In the initial request, the requester may also include any other identifying data that the requester may wish to furnish to assist the FBI in making a reasonable search. The request should include a return address for use by the FBI in responding; requesters are also encouraged to include a telephone number to facilitate FBI contacts related to processing the request. A determination of whether a record may be accessed will be made after a request is received.

CONTESTING RECORD PROCEDURES:

The Attorney General has exempted this system of records from the notification, access, amendment, and contest procedures of the Privacy Act. These exemptions apply only to the extent that the information in this system is subject to exemption pursuant to 5 U.S.C. 552a(j) or (k). Where compliance would not appear to interfere with or adversely affect the purposes of the system, or the overall law enforcement/intelligence process, the applicable exemption (in whole or in part) may be waived by the DOJ in its sole discretion.

Individuals desiring to contest or amend information maintained in the system should direct their requests according to the RECORD ACCESS PROCEDURES paragraph above, stating clearly and concisely what information is being contested, the reasons for contesting it,

and the proposed amendment to the information sought. The envelope and letter should be clearly marked "Privacy Act Amendment Request" and comply with 28 CFR 16.46 (Request for Amendment or Correction of Records). Some information may be exempt from contesting record procedures as described in the EXEMPTIONS PROMULGATED FOR THE SYSTEM paragraph, below. An individual who is the subject of a record in this system may amend those records that are not exempt. A determination whether a record may be amended will be made at the time a request is received.

NOTIFICATION PROCEDURES:

Same as RECORD ACCESS PROCEDURES paragraph, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

The Attorney General has exempted this system from subsections (c)(3) and (4); (d); (e)(1), (2), (3), (4)(G), (H), and (I), (5), and (8); (f), and (g) of the Privacy Act, 5 U.S.C. 552a. These exemptions apply only to the extent that information in a record is subject to exemption pursuant to 5 U.S.C. 552a(j) and/or (k). Revisions to the previously enacted rules in 28 CFR 16.96 (g-i) are being proposed in accordance with the requirements listed in 5 U.S.C. 553(b), (c), and (e) and published in the Federal Register. In addition, the DOJ will continue to assert all exemptions claimed under 5 U.S.C. 552a(j) and/or (k), or other applicable lawful authority, by an originating agency from which the DOJ obtains records, where one or more reasons underlying an original exemption remain valid. A determination of whether a record will be exempted will be made at the time a request for notice, access, and/or correction is received.

HISTORY:

National Crime Information Center (NCIC), JUSTICE/FBI-001, 64 FR 52343 (Sept. 28, 1999), as amended by 66 FR 8425 (Jan. 31, 2001), and 82 FR 24147 (May 25, 2017).

[FR Doc. 2019-19449 Filed: 9/9/2019 8:45 am; Publication Date: 9/10/2019]