Federal Bureau of Investigation

Privacy Impact Assessment
for the
Uniform Crime Reporting (UCR) System

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

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

Date approved: [February 8, 2023]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The U.S. Department of Justice (DOJ) Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Division Uniform Crime Reporting (UCR) Program is a collective effort on the part of federal, state, city, county, university/college, tribal, and territorial law enforcement agencies to voluntarily report crime and administrative law enforcement data to present a nationwide view of crime and law enforcement statistics. The CJIS Division maintains the UCR System which contains select information provided to the UCR Program; specifically, National Incident-Based Reporting System (NIBRS) crime information, the number of Law Enforcement (LE) Employees as of October 31 Data Collection, and UCR Program Profile information for state and domain UCR programs.[1] In addition, the UCR System maintains contact and audit log information for its users. The UCR System receives NIBRS and LE Employee information directly from state and domain UCR Programs and from contributing agencies via the NIBRS Collection Application (NCA) within the Collection of Law Enforcement and Crime Tool (COLECT).[2] The FBI releases statistical information from the UCR System via the Crime Data Explorer (CDE), an interactive online tool that enables law enforcement and the public to use and understand collected UCR data.

This Privacy Impact Assessment (PIA) addresses the privacy risks and mitigations associated with the collection and maintenance of point of contact and user information, the ability to link incident-specific data elements to individuals, and the release of UCR data through the CDE.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The FBI's UCR Program serves as the national repository for the collection of crime and law enforcement statistics. Its primary objective is to generate reliable information for use in law enforcement administration, operation, and management. The FBI's UCR Program has been the starting place for law enforcement executives, students of criminal justice, researchers, members of the

[1] The UCR Program also manages the National Use-of-Force Data Collection, the Law Enforcement Public Contact data collection, the Law Enforcement Officers Killed and Assaulted (LEOKA) data collection, LEOKA Health-Related Deaths, and the Law Enforcement Suicide Data Collection. Although the UCR Program manages these data collections, they are not maintained in the UCR System. These data collections have separate privacy documentation.
[2] COLECT has separate privacy documentation.

media, and the public at large seeking information on crime in our nation. User and stakeholder engagement has suggested a great desire and demand for reliable, consistent statistical data concerning crime that support a fundamental goal of comparability between crime areas over time. The focus on comparability holds whether the comparison may be implicit in the allocation of federal and state funding for criminal justice programs, explicit in the evaluation of the effectiveness of local law enforcement initiatives or state policy changes, or simply in the diagnosis of emerging problems by the media, researchers, or the public. Another common and critical use of crime data is its increasing use as a tool for accountability by law enforcement agencies in administering their own daily operations, and by advocacy groups and the public. The UCR Program provides an assessment of crime that is not available elsewhere in the criminal justice system. It is the largest compilation of crime statistics submitted by law enforcement agencies, covering approximately 95 percent of the nation's population. By providing this information to all levels of law enforcement, the UCR Program assists the FBI in meeting its mission to reduce criminal activity. Over the years, UCR data has become one of the country's leading social indicators for crime trending in the United States. The American public relies on UCR data sets for information on the fluctuations in the level of crime from year to year. Criminologists, sociologists, legislators, municipal planners, the media, and other students of criminal justice use the data for varied research and planning purposes.

In support of the UCR Program, the UCR System currently maintains information submitted to the NIBRS, the LE Employee Data Collection, state and domain UCR program profiles, and user information for UCR System users.

NIBRS

Law enforcement agencies (LEAs) throughout the country participating in the NIBRS voluntarily submit to the FBI's UCR Program crime data related to criminal offenses known to law enforcement and reports on persons arrested by LEAs. The NIBRS collects data on each single incident and arrest within 28 offense categories made up of 58 data elements, and arrest only information on an additional 10 offenses. These offenses are defined according to criteria established by the FBI's UCR Program, Congressional mandates, and through coordination with the law enforcement community via the FBI's CJIS Advisory Policy Board (APB). Through specific data elements in NIBRS, the FBI collects information about hate crimes, cargo theft, human trafficking, animal cruelty, and assaults on law enforcement officers. NIBRS incident submissions do not contain directly identifying information about offenders and victims (such as name); however, they do include general demographic information and other details that could potentially link a NIBRS incident to specific individuals. The UCR System stores NIBRS data, which is used to generate crime statistics for the use in law enforcement administration, operation, and management. NIBRS incident information is aggregated for statistical publication, but, except for select data elements, all incident data is available to the public through downloadable master files. More information about the FBI's UCR Program and the NIBRS is available at https://ucr.fbi.gov.

LE Employee Data Collection

The LE Employee Data Collection is an annual compilation of information that includes details on the sworn or civilian status and gender of law enforcement agency staff. The data collection provides the FBI UCR Program with a yearly total numeric count by race and ethnicity of full-time, part-time, and reserve/auxiliary/other sworn male, female, and non-binary law enforcement officers, and full-time, part-time and reserve/auxiliary/other male, female, and non-binary civilian employees as of October 31 of the reporting year.

UCR Program Profiles

The state/domain UCR program profiles contain comprehensive data about each state/domain UCR program. All fifty states in the nation have their own UCR program, which streamlines the collection of UCR data from local law enforcement agencies, ensures consistency and comparability of data, and provides a higher quality of service to the law enforcement community. Establishment of a UCR program is not limited to state governments. Federal, tribal, and territorial agencies may also institute UCR programs, referred to in this document as domain UCR programs. Domain UCR programs gather crime information from the law enforcement agencies under their domain and forward the data to the FBI. The UCR Program Profiles are a resource that both the FBI and the state/domain programs can use to track compliance with FBI data processes, procedures, and implementation of new initiatives; to determine if training and auditing programs are in place; and to capture information on data submissions, data quality, and other pertinent information. These documents also allow state/domain UCR programs to assist one another in addressing areas of concern. UCR program profiles include point of contact (POC) information for state and domain UCR programs.

Providing Information to the UCR System

The UCR System contains information submitted to the FBI's UCR Program by law enforcement agencies. The majority of law enforcement agencies submit data through their state/domain UCR programs. All FBI UCR Program participants submit data to the UCR System electronically. The FBI's UCR System accepts NIBRS and LE Employee submissions via flat file data submissions, web services (machine-to-machine transmission), and submissions to the NIBRS Collection Application (NCA) and LE Employee report form on COLECT.

For flat file submission of NIBRS data, agencies use three types of electronic flat files to forward data to the FBI:

- The Group A Incident Report provides all the information about Group A offenses using up to six data segments (Administrative, Offense, Property, Victim, Offender, and Arrestee). Each segment is discussed in greater detail in Section 3 below.
- The Group B Arrest Report supplies data concerning each arrestee for a Group B offense via the arrestee segment.
- The Zero Report indicates that no criminal activity occurred within an agency's jurisdiction during a given month.

The three flat file submissions use a series of established data elements (i.e., data fields within each segment) to describe the details of each component of the crime. For each data element, reporting agencies may choose the most appropriate data value (i.e., a specific code representing one of the acceptable entries for each data element).

State/domain UCR programs also submit NIBRS data through secure file transfer protocol (SFTP) and web services, which are automated processing. The SFTP uses the Enterprise File Transfer Service (EFTS) offered by the CJIS Division as a platform for agencies to upload UCR submissions, which are then downloaded by UCR Program staff and imported into the UCR System. State/domain

UCR programs also use web services to send UCR submissions via a machine-to-machine interaction. Web services use private/public key certifications to authenticate state/domain program system transmissions of UCR submissions to CJIS Division servers. Once received on CJIS Division servers, the submissions are pushed to the UCR System.

Agencies may manually provide NIBRS incidents and LE Employee counts to the UCR system through the NCA and LE Employee report form on COLECT. The NCA allows agencies with small staff and/or light yearly caseloads to manually submit NIBRS incidents to the UCR System. The LE Employee report form in COLECT similarly allows agencies to report their LE Employee Data Collection counts. To submit data through COLECT, agencies log in to the Law Enforcement Enterprise Portal (LEEP)[3] and navigate to the COLECT platform. Once logged in to COLECT, users choose the NCA or the LE Employee report form and then manually enter their incident or count information. COLECT submits data to the UCR System via web services (a machine-to-machine interaction) for processing, retention, and publication. Web services uses private/public key certifications to authenticate the transmission of data from the COLECT to the UCR System. Through COLECT users will also receive messages from the UCR System regarding data submissions, such as error and reject messages, data quality messages, and other messages regarding agencies' data submission statuses.

State/domain UCR programs provide POC information and other agency reference information for the UCR program profiles via email. FBI personnel manually upload the UCR program profile information to the UCR System.

Managing Data in the UCR System

The FBI developed a web user interface, known as the UCR Dashboard, to enable both FBI UCR Program staff and external stakeholders to log in to the UCR System and manage UCR data. NIBRS incidents and LE Employee data submitted to the UCR System pass through certain criteria for entry to check the data for reasonableness, quality, and validity.[4] Users access the UCR Dashboard via LEEP. Once logged in to the UCR Dashboard, users leverage dashboards and data management tools. Through the data management tools, users can see any data errors identified by the UCR System. The UCR Dashboard provides a mechanism for the FBI UCR Program staff to work directly with data contributors to audit the data and resolve any quality concerns, as needed. State/domain UCR programs may also submit data through the UCR Dashboard via flat file submissions.

For external users, the UCR Dashboard provides a read-only platform through which they can view and manage their UCR data submitted through COLECT, web services, or flat file submission. The users, whether internal or external to the FBI, can view UCR data for the last 5 years. Furthermore, the UCR Dashboard hosts Role and Agency Management data which is visible and contains limited personally identifiable information (PII) on its users and agency specific information. For Agency Management, the UCR Dashboard captures agency reference information (e.g., agency

[3] LEEP is a federated gateway that securely connects law enforcement, criminal justice, and homeland security communities to applications and services over the Internet. The benefits of LEEP include a single sign-on for users to access various services and systems and ensuring that only authenticated users have access to those systems and services. LEEP has separate privacy documentation.
[4] For more information on UCR data quality guidelines, please visit https://ucr.fbi.gov/data-quality-guidelines-new.

name, associated originating agency identifiers (ORIs), agency type, judicial district code), population data, NIBRS Transition Details, and NIBRS Start Date.

Users can retrieve their submitted data by any data element. FBI UCR Program users have access to all data submitted to the UCR System. The UCR system allows FBI users to run reports based on agency, data field, or date of an incident. FBI users can export data for publication. External users (state/domain UCR program users and LEA users) can review UCR data by logging in to the UCR System web interface and accessing the UCR dashboard.

Public Release of UCR Data

Once all data quality concerns are resolved and the FBI's UCR Program clears data for release, statistical data is published on the CDE. The CDE is a web-based solution to publicly share comprehensive, timely, and accurate statistical crime and law enforcement data submitted by law enforcement agencies. The CDE provides public access to FBI UCR Program statistical data, traditional publications, and master files. The CDE is an interactive tool enabling the user to more easily consume the massive amounts of data collected and published by the FBI's UCR Program. Through the CDE, the public can search, view, and export data collected by the UCR Program. The CDE is available at https://cde.ucr.cjis.gov.

To publish data on the CDE, FBI UCR Program staff extract the data from the UCR System and upload it to the CDE. NIBRS information displayed through the CDE can be searched by crime type, location (national, state, agency), and year. The CDE displays statistical crime data via national estimates and crime trends at the state and national level for violent crime and property crime and offense counts by year at the agency level. CDE also displays NIBRS-reported information regarding offender and victim demographics. The CDE has separate statistical pages for hate crime, expanded homicide data, expanded property crime, arrest, police employment, law enforcement officers killed and assaulted, and use of force data. Other datasets shown on the CDE include agency participation, cargo theft, and human trafficking. In addition to the data views available on CDE, downloadable editions of the traditional publications available on FBI.GOV from 2020 and beyond have been migrated to the CDE documents and downloads area.

The CDE provides select datasets and master files for download. Incident-based data by state, summary data estimates, and data about other specific topics may be downloaded in common separated value (CSV) files. Data are also available via the Crime Data application programming interface (API), a read-only web service that returns JavaScript object notation (JSON) or CSV data. The CDE provides a feedback link through which users can anonymously provide suggestions for improving the CDE. The feedback suggestions are available for the FBI to review but are not maintained within the CDE or the UCR System. The CDE also provides a link to a "contact us" webform. The webform allows individuals to email questions to the UCR Program. Although the CDE provides a link to the webform, the webform and any responses from the UCR Program are not stored in the CDE or the UCR System.

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

Authority	Citation/Reference

X	Statute	28 U.S.C. § 534; 34 U.S.C. § 12532; 34 U.S.C. § 41303; 34 U.S.C. § 41305; 34 U.S.C. § 41309; Anti-Arson Act of 1982, Pub. L. No. 97-298, § 3, 96 Stat. 1319 (1982); USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 307 (e), 120 Stat. 240 (2006)
	Executive Order	
X	Federal Regulation	28 CFR 0.28(f)
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

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

As discussed above, the UCR System contains NIBRS incident submissions, state/domain UCR program POC information, numeric counts collected through the LE Employee data collection, and user information and audit logs for UCR System users.

NIBRS currently collects incident and arrest information from law enforcement agencies for 28 Group A offense categories that include 71 Group A criminal offenses. The data elements collected for reported NIBRS offenses are divided in to six segments: Administrative, Offense, Property, Victim, Offender, and Arrestee.

The **Administrative Segment** includes information about the agency reporting the incident and general information about the incident, such as date and time it occurred and whether law enforcement has cleared the incident.

The **Offense Segment** includes information about the crimes committed during the incident and the circumstances surrounding the incident, such as the type of location at which the incident occurred, whether force was used during the incident, whether drugs or alcohol were involved, and, if the incident is determined to be a hate crime, the offender's bias motivation.

The **Property Segment** describes the type of property loss, recovery, seizure, or damage that occurred during an incident.

The **Victim Segment** includes general demographic information about the victim(s) involved in the incident, such as the victim's age, sex, race, and ethnicity. The victim segment also captures the

type of victim (e.g., individual, business, society/public, law enforcement officer); whether the victim was injured; and the relationship(s) of the victim to the offender(s) (e.g., spouse, child, friend, employer). If the victim was a law enforcement officer, the victim segment also collects information about the officer's activities and assignment at the time of the incident. The victim segment does not collect directly identifying information about the victim such as name or date of birth.

The **Offender Segment** includes general demographic information about the offender such as the offender's age, sex, race, and ethnicity. The offender segment does not collect directly identifying information about the offender such as name or date of birth.

The **Arrestee Segment**[5] includes demographic information about individuals arrested for the reported incident, such as age, sex, race, and ethnicity, and general information about the circumstances surrounding the arrest (e.g., whether the arrestee was involved in multiple incidents or whether the arrestee was armed at the time of the arrest). The arrestee segment does not collect directly identifying information about the arrestee such as name and date of birth.

A complete list of all data elements collected by NIBRS, including a definition of each data element and offense, is available in the *NIBRS User Manual*, https://ucr.fbi.gov/nibrs/nibrs-user-manual. Any decision regarding changes to the information collected by NIBRS, such as the collection of additional offenses or data elements, is made by the FBI in consultation with federal, state, local, tribal, and territorial law enforcement agencies through the CJIS APB process. Once approved, changes in the data collection are added to the *NIBRS User Manual*.

POC information within the UCR program profiles includes the names, phone extensions, and email addresses of the FBI employees who support the specific state/domain UCR program; the name, agency affiliation, address, phone number, fax number, and email address of the POC for the state/domain program; the name of the CJIS System Officer[6] applicable to the state/domain program; and a link to the state/domain program's website, if applicable.

For role management in the UCR System, the UCR System collects a user's first and last name, LEEP user ID, agency email address, agency address, agency telephone number, employer/agency name and ORI, type of employing agency, and user role within the UCR System.

The CDE does not collect any information on individuals visiting the public website other than general numeric counts of the number of visitors to the site and general patterns in users' behavior over time (e.g., which parts of the site users are visiting and which data sets users are downloading).

---

[5] For Group A offenses, an agency cannot submit an Arrestee Segment without the Administrative, Offense, Property (if applicable), Victim, and Offender Segments. Currently, for Group B offenses, only the arrestee segment is reported.
[6] A CJIS Systems Officer is a duly authorized official of a federal, state, local, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to their criminal justice users with respect to the criminal justice information from various systems managed by the FBI CJIS Division.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	The UCR System only contains names for state/domain program and FBI POCs and UCR System users. NIBRS collects only general demographic information for offenders, victims, and arrestees.
Date of birth or age	X	A, B, C, D	NIBRS collects the age of victims, offenders, and arrestees involved in NIBRS incidents. NIBRS does not collect full dates of birth.
Place of birth			
Gender	X	A, B, C, D	NIBRS collects the gender of victims, offenders, and arrestees involved in NIBRS incidents. The LE Employee collection includes the number of employees at a law enforcement agency by gender.
Race, ethnicity or citizenship	X	A, B, C, D	NIBRS collects the race/ethnicity of victims, offenders, and arrestees in NIBRS incidents. The LE Employee collection includes the number of employees at a law enforcement agency by race and ethnicity.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)			
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Work mailing address	X	A, B, C, D	Applies to UCR System users and State/domain UCR Program contacts
Work e-mail address	X	A, B, C, D	Applies to UCR System users and State/domain UCR Program contacts
Work phone number	X	A, B, C, D	Applies to UCR system users and State/domain UCR Program contacts
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A, B, C, D	If law enforcement officer is chosen as the victim type for a NIBRS incident, NIBRS will collect the victim officer's assignment.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)	X	A, B, C, D	The UCR Program Profiles contain the website of the state/domain UCR programs.
Foreign activities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C, D	NIBRS collects information about criminal incidents when they become known to law enforcement.
Juvenile criminal records information	X	A, B, C, D	NIBRS collects information about criminal incidents when they become known to law enforcement. This includes incidents with juvenile offenders.
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C, D	NIBRS collects the location type at which a criminal incident occurs (e.g., hospital, store, residence), but does not collect the actual address at which a criminal incident occurs.
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
System admin/audit data:	X	A, B, C, D	The UCR System logs a user session from start to finish. The CDE maintains audit logs only for access to the system infrastructure for the operations and management of the CDE; therefore, the CDE audit logs contain information only on FBI contractors and personnel.
- **User ID**	X	A, B, C, D	
- **User passwords/codes**			
- **IP address**	X	A, B, C, D	This applies to the IP address through which UCR System users access the UCR System or the back-end infrastructure of the CDE. The CDE does not track IP addresses of individuals accessing the public website.
- **Date/time of access**	X	A, B, C, D	
- **Queries run**	X	A, B, C, D	Queries are collected in audit tables. If a file is accessed, the system would not necessarily generate a log, but the file may not be modified or downloaded without a log being generated.
- **Content of files accessed/reviewed**			
- **Contents of files**	X	A, B, C, D	

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	ORI; type of employing agency; user role; Arrestee Sequence Number; Arrest Transaction Number Users will receive messages and notifications from the UCR System regarding data submissions, such as error and reject messages, data quality messages, and other messages regarding agencies' data submission statuses.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax		Online	X
Phone		Email	X		
Other (specify): Users apply for access to the UCR Dashboard online. NIBRS information is not obtained directly from the individual about whom the information pertains. Rather, data elements are obtained by law enforcement agencies and submitted to the FBI by the agencies or through the agencies' respective state/domain programs. The UCR System and UCR Dashboard receive user information from LEEP. State/domain UCR programs email POC information and other profile information to the UCR Program staff.					

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

Non-government sources:

Members of the public	X	Public media, Internet		Private sector	
Commercial data brokers					
Other (specify): The CDE includes a feedback tool that allows any individual using the CDE to provide recommendations on how to improve the application. Members of the public may provide feedback; however, the feedback tool does not solicit any PII, and individuals providing feedback are asked not to include any PII or sensitive information. The CDE also includes a link for individuals to contact the UCR Program. Information submitted through the "contact us" link does not reside in the UCR System or the CDE.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	FBI personnel with access to the UCR System have access to all data in the system.
DOJ Components	X	X	X	For data submitted through COLECT, DOJ components have direct access to data they submitted via the NCA or the LE Employee report form. DOJ users of the UCR Dashboard have access to the data associated with their assigned ORIs. DOJ components can download available master files via the CDE.
Federal entities	X	X	X	For data submitted through COLECT, Federal entities have direct access to data they submitted via the NCA or the LE Employee report form. Federal users of the UCR Dashboard have access to the data associated with their assigned ORIs. Federal users can download available master files via the CDE.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
State, local, tribal gov't entities	X	X	X	For data submitted through COLECT, state, local, and tribal government entities have direct access to data they submitted via the NCA or the LE Employee report form. State, local, and tribal users of the UCR Dashboard have access to the data associated with their assigned ORIs. State, local, and tribal users can download available master files via the CDE.
Public		X		The UCR System pushes information to the CDE for public release.
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

As discussed in Section 2.1, law enforcement agencies and state/domain UCR programs submit data to the UCR System. Internal FBI users have direct access to the UCR System. Internal users consist of the FBI's UCR Program Office and the FBI's CJIS Division Information Technology Management Section (ITMS) development and operations and maintenance teams. Users log in to the UCR System via LEEP. Internal users have access to all information in the UCR System and can upload new data received from the state/domain programs to the UCR System.

External users have read-only access to the UCR System via the UCR Dashboard, which allows them to view and manage data they submit to the UCR System. External users consist of state/domain UCR Programs and agencies submitting information to the UCR System. To access the UCR Dashboard, users apply for access via the UCR Dashboard icon on LEEP. The FBI's UCR Program controls initial UCR Dashboard account access for agencies. Once the UCR Program establishes an agency point of contact in the UCR Dashboard, the point of contact is assigned an Administrator role and the appropriate ORIs associated with the user's area of responsibility. Administrators serve as account managers for their agencies. As account managers, Administrators can create, approve, update, and delete roles and privileges for their users and assign roles to users (i.e., other administrators or reviewers). Administrators also have the functionality assigned to a

reviewer role and can view the transaction history for any incidents associated with their assigned ORIs. Reviewers can view the transaction history for data submitted by their assigned ORIs. All agency users will be able to download a copy of their submissions.

FBI personnel supporting the UCR Program and UCR Dashboard have access to information through the Administrator role. FBI personnel supporting UCR data collections can view all entries within the system; view the transaction history for data; and create, approve, update, and delete user accounts. Only FBI Administrators can view the UCR Dashboard audit logs.

Database administrators are responsible for maintaining the database and can view and access the data in the UCR Dashboard database. System administrators are responsible for maintaining the software, security, and computers.

Access to a specific user's information is role based and restricted to the user, other users in the user's chain of review, and FBI personnel supporting the UCR Dashboard and the UCR Program, including system and database administrators. User information is maintained to provide users and reviewers with point of contact information, to facilitate generating system reports on items such as which users and agencies have submitted data and which users and agencies have data that need to be reviewed or submitted, and to allow users to subscribe to system reports and alerts. The FBI will also leverage user information to provide messages from the UCR Dashboard such as data submission errors, data quality messages, and other messages regarding agencies' data submission statuses.

Account request forms will be stored in user tables within the UCR Dashboard and are only accessible to FBI system administrators and users assigned the Administrator role. Agency Administrators can only access the account request forms for their assigned ORIs.

Authorized users log in to the UCR Dashboard via LEEP, which authenticates the users. Once logged in to the UCR Dashboard, it controls the authorization/roles and data access controls for the users. The users, based on assigned permissions, can submit, view, and download data associated with their ORIs and view error messages associated with their data. Users can view the data history (i.e., created, deleted) for all the data submissions associated with their ORIs. If a user is designated the Administrator role, the user can opt in to email notifications to be notified when other users within the Administrator's assigned ORIs request access to the UCR Dashboard and when a user profile is updated.

Authorized LEEP users may access POC information from the UCR program profiles within the UCR Program's JusticeConnect Community.[7] The UCR JusticeConnect Community is restricted, which means that users are vetted prior to receiving access.

Agencies that submit data via the NCA and the LE Employee report form in COLECT have direct access to their data submissions in COLECT. Based on the user's assigned permission, the user

[7] JusticeConnect is an online user-driven, real-time collaboration and communication tool. JusticeConnect promotes collaboration with and among the FBI's criminal justice partners by providing a real-time environment in which to communicate with experts, create and join communities of common interest, create blogs to present ideas and receive feedback, share files with colleagues, and exchange ideas through online forums. JusticeConnect has separate privacy documentation.

will be able to enter, view, and manage their submitted data. COLECT users can only access the incident data in COLECT associated with their agency's ORI. COLECT users do not have direct access to the UCR System or UCR Dashboard via COLECT. Through COLECT, they can only access their data they have submitted through COLECT.[8]

Audit logs for the UCR System, the UCR Dashboard, and the CDE are accessible only to a small subset of FBI's CJIS Division Information Technology Management Section (ITMS) system security administrators (SSAs) and Information System Security Officers (ISSOs) who monitor the audit logs for anomalies. SSAs monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days.

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

The FBI's UCR Program publicly releases aggregated statistical data from the UCR System via the CDE, available https://cde.ucr.cjis.gov. The CDE displays statistical graphs, charts, and tables for data submitted to the UCR Program. This includes statistical representations of NIBRS data and LE Employee data. After the FBI's UCR Program releases statistical information on the CDE, the public can also download UCR tables of statistical counts and master files from the CDE. The master files consist of the underlying data elements used by the UCR Program to publish aggregated statistical data. Master files currently exist for NIBRS data, LE Employee data, cargo theft data, and hate crimes data. For the NIBRS master files (including cargo theft and hate crimes), the incident number and arrestee number are masked, but all other data elements are provided. UCR Program Profiles are not publicly available; however, general contact information for state/domain UCR programs is available on fbi.gov.

The FBI's UCR Program's publications and statistical information displayed on the CDE aggregate the data submitted to the UCR Program to provide an overall view of crime trends at a national, state, or agency level. The FBI designs the CDE's charts, graphs, and tables to provide an overarching statistical view of the data rather than incident level specifics. However, the need of the law enforcement executives, students of criminal justice, researchers, members of the media, and the public at large to understand crime in the United States requires the release of the underlying data used for the FBI statistical displays. Consequently, for research and statistical analysis purposes, after the FBI UCR Program publishes its statistical data, the FBI's UCR Program releases master files to the CDE for public download. The master files contain incident level submissions to the FBI's UCR Program; however, they do not contain any information directly identifying individuals. To restrict the public's ability to link a specific incident submission to an incident or arrest report from a submitting agency, the incident number and arrestee number that correspond with law enforcement agencies' records are masked. Nothing in the NIBRS master file can confirm that specific data elements correspond with a specific offender, arrestee, or victim. Section 8 further discusses the privacy risks

[8] COLECT has separate privacy documentation which explains user roles within COLECT.

with releasing the master files.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

UCR Dashboard User Information: The account request form for access to the UCR Dashboard on LEEP includes a Privacy Act statement informing potential users of the purpose for collecting their information and how it will be used.

The state/domain UCR programs submit their business and individual POC information voluntarily and understand via participation in the FBI's UCR Program the purpose of providing their information and how it will be used.

The UCR System collects NIBRS data elements from law enforcement agencies that describe criminal incidents and numeric counts of LE Employee demographics. These data elements do not directly identify anyone involved in the incident or LE employees. NIBRS data elements contain information intended to describe, in a de-identified way, information about the crime incident. The data elements are submitted by law enforcement agencies rather than the individuals involved in the incidents; therefore, the FBI does not provide any direct notice to individuals that their de-identified data may be submitted to the FBI's UCR Program. This Privacy Impact Assessment provides general notice to the public about the type of information collected, maintained, and disseminated by the UCR System.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

The UCR System collects data elements from law enforcement agencies that describe reported criminal incidents. These data elements do not directly identify anyone involved in the incident. Submitting law enforcement agencies determine which incidents to report, not the individuals involved in the incidents. The FBI does not provide individuals involved in such incidents the opportunity to decline to provide information to the UCR System because those individuals are not directly providing information to the UCR System.

Use of the UCR Dashboard is voluntary. Individuals applying for access to and using the UCR Dashboard choose to provide their information to receive access. In addition, all UCR Dashboard users specifically agree to a government system notice informing them that they have no reasonable expectation to privacy regarding their activities on a government system and that their use of the government system may be monitored, intercepted, searched, and/or seized.

State/domain UCR programs voluntarily provide their business and individual contact information to the FBI UCR Program.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

NIBRS incident information submitted to the UCR System does not directly identify individuals. Similarly, the LE Employee data collection does not include directly identifying information, only numeric counts. Law enforcement agencies providing information to the FBI are responsible for ensuring its accuracy.

UCR Dashboard users and state/domain POCs may request access to their records by following the guidance provided on the FBI's website at *https://www.fbi.gov/services/records-management/foipa*. A request for access to a record from this system of records must be submitted in writing and comply with 28 CFR part 16. Individuals may mail, fax, or electronically submit a request, clearly marked "Privacy Act Access Request," to the FBI, ATTN: FOI/PA Request, Record/Information Dissemination Section, 200 Constitution Drive, Winchester, VA 22602-4693; facsimile: 540-868-4995/6/7; electronically: *https://www.fbi.gov/services/records-management/foipa/requesting-fbi-records*. 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.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The UCR System, UCR Dashboard, and the CDE currently operate under the ATO for the UCR System, which expires on November 18, 2025. In the future, the UCR System, UCR Dashboard, and the CDE will be incorporated into the Crime Data Value Stream (CDVS) security boundary which will provide information technology (IT) security controls to all systems and applications within its boundary. The FBI is currently working on the ATO for CDVS.

	If an ATO has not been completed, but is underway, provide status or expected completion date: **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** All the security controls relevant to the UCR System, UCR Dashboard, and the CDE using National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and FBI Office of Chief Information Officer (OCIO) policies have been reviewed and are continuously monitored in RiskVision. ISSOs conduct continuous evaluations, and monthly status reports are presented to the Assistant Section Chief of the Information Technology Management Section.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The UCR System underwent evaluation in February 2022. All identified critical and high vulnerabilities have been removed. Other vulnerabilities have been mitigated or placed on the Plan of Action and Milestones worksheet for further evaluation for removal or mitigation. ISSOs conduct continuous evaluations, and monthly status reports are presented to the Assistant Section Chief.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Audit logs are kept for one year. SSAs monitor audit logs on a daily basis. The ISSO reviews audit logs, at a minimum, every seven days. Security personnel review audit logs using automated log aggregation toolsets.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** For user reference, user guides and answers to frequently asked questions are available within the COLECT for the NCA and the LE Employee report form. The UCR Dashboard also includes frequently asked questions.

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

Threats to the UCR System and the UCR Dashboard include malicious/unauthorized acts by authorized users and possible unauthorized external malicious users. Security controls have been implemented to minimize the risk. Only FBI personnel and authorized external users have direct

access to the UCR System and the UCR Dashboard. Access to the CDE system infrastructure is restricted to FBI contractors and personnel supporting the FBI's UCR Program. All UCR System and UCR Dashboard users are required to be trained on the proper use of the systems. Access is role-based as explained in Section 4.1. External users have read-only access to the UCR Dashboard. Only a small subset of FBI users can actually edit the data within the UCR System. Web session logs and Oracle tables have audit logs to track changes to information within the UCR System and the UCR Dashboard.

Mitigation of potential unauthorized or inappropriate access to the UCR System and UCR Dashboard relies on system security that ensures only authorized users have access to the UCR System and UCR Dashboard. Users access the UCR System and UCR Dashboard via LEEP which requires multi-factor authentication for log on. Role-based controls and access control list(s) at the group and individual level further protect the information in the UCR System and UCR Dashboard. Web services use private/public key certifications to authenticate state/domain program system transmissions of UCR submissions to CJIS Division servers.

All users are notified, through warning banners and by signing the *FBI Rules of Behavior* or the *LEEP Rules of Behavior* that they are subject to periodic, random auditing of the searches they performed, when they performed the searches, and what data was accessed or altered. This awareness discourages unauthorized or non-work-related searching and provides awareness of data that has specific handling requirements or sensitivity. The UCR System and UCR Dashboard also maintain audit logs that record the User ID of individuals accessing the system and time-stamped events such as attempted logins/logouts and system configurations. Anomalous behavior or misuse of the UCR System or UCR Dashboard is subject to investigation and appropriate sanction, ranging from denial of access and elimination of privileges to referral to the FBI's Inspection Division, Internal Investigations Section, for investigation of FBI employee misconduct. Audit data from the UCR System and the UCR Dashboard is supplied to the FBI's Enterprise Security Operations Center, which has a centralized view that can correlate audit information from different FBI systems.

All individuals with access to the UCR System, the UCR Dashboard, and the CDE system infrastructure must comply with applicable security and privacy protocols addressed in the *CJIS Security Policy* (available at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view), the *CJIS User Agreement*, and the *LEEP Rules of Behavior*. UCR System and UCR Dashboard users acknowledge that they understand sanctions may be applied for intentional misuse of the UCR System and UCR Dashboard. General users must be knowledgeable of the security practices for general users and the privileged user must be knowledgeable of the security practices for privileged users.

UCR Operations staff, ISSOs, and the SSA continually review the IT security controls per FBI policy and also use the NIST special publication 800-53A, revision 5 for expended definition and guidance. The ISSO is required to review security controls annually. Risk Assessments focuses on assessing risk to reduce the risk of unauthorized access, use, and disclosure. The risk assessment is reviewed and updated at least annually. Confidentiality is protected through acceptable security controls addressing boundary protection/external telecommunication, transmission confidentiality and integrity, and remote access/protection of confidentiality and integrity using encryption.

The UCR System, the UCR Dashboard, and the CDE reside in the AWS Gov-Cloud

environment. Access to FBI infrastructure in the cloud infrastructure is limited to FBI personnel and appropriately cleared AWS personnel. Access by FBI personnel to specific FBI applications and datasets are determined at the application and dataset level. Both the FBI and AWS collect and maintain audit logs and user login identifiers; however, AWS personnel cannot access FBI applications or datasets or the audit user activity therein. Data in transit is encrypted using Transport Layer Security Federal Information Processing Standard 140-2 encryption, and all interconnections between the AWS Gov-Cloud and the FBI use firewalls and security filtering. The UCR System, UCR Dashboard, and CDE are logically separated from non-FBI data and are located in a virtual private cloud of AWS Gov-Cloud managed by the FBI.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Information collected and published by the FBI's UCR Program is maintained in accordance with the record retention schedules approved by the National Archives and Records Administration: job number N1-065-07-22, available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-07-022_sf115.pdf; and job number N1-065-09-23, available at https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-09-023_sf115.pdf. Master files and UCR publications are maintained permanently. Audit logs are maintained for up to two years.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. ___X__ Yes.

This applies to UCR System and UCR Dashboard user information and state/domain UCR program profile and contact information. NIBRS information and LE Employee Data Collection information cannot be retrieved by personal identifier. Information can be retrieved from the UCR System by any collected data element. None of the data elements in the NIBRS directly identify an individual. UCR Program Profile information may be searched by name or other identifier. Information displayed through the CDE may be searched by crime type, location (national, state, agency), and year. Within the COLECT, users can only query NIBRS incidents associated with their ORI by incident number and incident date. Audit logs for the UCR System, UCR Dashboard, and the CDE may be retrieved by username or other personal identifier.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

Audit logs for the UCR System, UCR Dashboard, and the CDE system infrastructure are covered by *Department of Justice Information Technology, Information System, and Network Activity and Access Records*, **DOJ-002**, 86 Fed. Reg. 132 (Jul. 14, 2021). UCR Program Profile contact

information and UCR Dashboard user information is covered by *Bureau Mailing Lists*, **JUSTICE/FBI-003**, 70 Fed. Reg. 7513 (Feb. 14, 2005), as amended at 82 Fed. Reg. 24147 (May 25, 2017); and *FBI Online Collaboration Systems*, **JUSTICE/FBI-004**, 82 Fed. Reg. 57291 (Dec. 2, 2017).

NIBRS incident data and LE Employee data submitted to the FBI's UCR Program and available through the CDE does not create a system of records because the incident data does not contain names or other identifying information on individuals and is therefore not retrieved from the system by the name or identifying number, symbol, or particular assigned to a specific individual.

Section 8: Privacy Risks and Mitigation

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

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

The FBI's UCR Program compiles data on crimes known to law enforcement; consequently, the data is collected from law enforcement agencies rather than offenders or victims involved in criminal incidents. Because the information is collected from law enforcement agencies throughout the nation, there is a risk that incidents in one location may be reported differently than incidents in another location. To mitigate this risk, the FBI's UCR Program has extensive user manuals (available at https://ucr.fbi.gov/user-manuals) that provide guidance to law enforcement agencies on how to report incidents to the FBI's UCR Program. The FBI's UCR Program also provides training to law enforcement agencies on the appropriate categorization of incidents for FBI UCR Program purposes. In addition, once the data is submitted to the FBI's UCR Program, the FBI's UCR Program staff review the data to determine adherence to UCR policy, conformance to UCR definitions and principles, and consistency with established statistical methodologies and norms. FBI UCR Program staff review the data through a series of multi-layered processes to check the data for reasonableness, quality, and validity. For more information on UCR data quality guidelines, please visit https://ucr.fbi.gov/data-quality-guidelines-new.

The greatest privacy vulnerability created by the collection of the UCR data exists in the possibility of linking incident-level NIBRS data with knowledge of the incident from outside sources of information to identify the offenders or victims involved in an incident. Given the data elements collected by NIBRS, the possibility exists that incident-level NIBRS data, when linked with other

sources of information such as media accounts, may allow someone to link identifying information in other sources of information to offender and victim data elements within the NIBRS master file. For example, if the incident involves a homicide reported by law enforcement in a community that only had one homicide for a given month, the possibility exists that someone could link the agency's incident-level NIBRS data submission to a media report regarding the homicide and thereby identify the offender and victim that correspond with the data elements submitted to the UCR Program. To mitigate the privacy impact to the extent possible, the FBI's UCR Program collects only those data elements that are necessary to provide law enforcement and the nation with a comprehensive picture of crime in the United States. The data elements collected about offenders and victims contain only basic demographic information necessary to analyze crime trends. Any proposals for the collection of additional data elements or offenses are vetted through the CJIS APB process to provide law enforcement agencies and state/domain programs with the opportunity to express any concerns with the collection of additional information. The UCR Program publications and statistical information displayed on the CDE aggregate the data submitted to the UCR Program to provide an overall view of crime trends at a national, state, or agency level. In addition, the incident number and arrestee number that correspond with law enforcement agencies' records are not publicly available through the NIBRS master file. Therefore, although someone could reasonably assume that a specific incident may correspond with a specific media account, nothing in the NIBRS master file can confirm that specific data elements correspond with a specific offender or victim.

Agencies participate in the FBI's UCR Program with the understanding the information submitted to the program will be shared with the public. Agencies have the option to, and have on occasion, withheld or deferred reporting incidents they have determined to be too sensitive for public release or which are still under investigation. In addition, agencies may also use general descriptions such as other or unknown for data elements which the agency believes should not be shared.

The only directly identifiable information contained within the UCR system is POC information for FBI personnel, POC information for state/domain UCR programs, and user information for the UCR System and UCR Dashboard. POC information contains only names, phone numbers, email addresses, and general business contact information for the state/domain UCR programs. Similarly, user information in the UCR System and UCR Dashboard is limited to basic contact information needed to authenticate its users (e.g., name, LEEP user ID, agency email address, agency address, agency telephone number, employer/agency name and ORI). Direct access to the UCR System and UCR Dashboard is restricted to FBI contractors and personnel and authorized external users, and POC information for individuals within a state/domain UCR program is only shared within the FBI, with UCR System users, or with authorized LEEP users.