U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

LAW ENFORCEMENT RECORDS MANAGEMENT SYSTEMS (RMSs)

as They Pertain to FBI Programs and Systems

Integrated Automated Fingerprint Identification System (IAFIS):
Next Generation Identification (NGI)
Interstate Identification Index (III)

National Crime Information Center (NCIC)

The Law Enforcement National Data Exchange (N-DEx)

National Instant Criminal Background Check System (NICS)

Uniform Crime Reporting (UCR) Program:
Summary Reporting System
National Incident-Based Reporting System (NIBRS)
Hate Crime Statistics Program
Law Enforcement Officers Killed and Assaulted (LEOKA) Program

This document replaces the *FBI's Manual of Law Enforcement Records*, 1984.

INTRODUCTION

The need for good record-keeping and information-sharing practices has taken on added significance in today's global environment. Not only do good records provide crucial internal information (i.e., business operations and case management support—not to mention the official memory of an agency's investigations), law enforcement agencies now need to communicate agency-to-agency and across continents in order to protect the Nation's citizens. Nothing is more important to accomplishing that mission than having accessibility to accurate and timely records. Calls for service records and investigative, arrest, criminal identification, detention, and even civil records hold information that by themselves mean little; however, when pieced together with information from other jurisdictions, the result can help with all levels of investigations and aid in safeguarding the Nation.

What this document provides

More than ever, the FBI is committed to helping law enforcement meet its ongoing need for immediate, accurate, and reliable information. One small way to achieve that goal is to provide in one document the information that agencies need to know about records management systems (RMSs) as they pertain to the programs and services that the FBI provides. This manual, *Law Enforcement RMSs (as They Pertain to FBI Programs and Systems)*, provides that guidance. The information in this publication addresses law enforcement record requirements for the FBI's:

- Integrated Automated Fingerprint Identification System (IAFIS)
  - Next Generation Identification (NGI)
  - Interstate Identification Index (III)
- National Crime Information Center (NCIC)
- The Law Enforcement National Data Exchange (N-DEx)
- National Instant Criminal Background Check System (NICS)
- Uniform Crime Reporting (UCR) Program
  - Summary Reporting System
  - National Incident-Based Reporting System (NIBRS)
  - Law Enforcement Officers Killed and Assaulted (LEOKA) Program
  - Hate Crime Statistics Program

What this document does not provide

This document is not designed to provide information on how to set up an RMS. There are several publications already available to assist agencies in that initial task. Two of these documents are:

- The Bureau of Justice Assistance's *Standard Functional Specifications for Law Enforcement Records Management Systems*, http://it.ojp.gov/documents/LEITSC_Law_Enforcement_RMS_Systems.pdf

- The International Association of Chiefs of Police (IACP)/Department of Justices' Community Oriented Policing Services (COPS) Technology Technical Assistance

Program's *Records Management Systems*,
http://www.iacptechnology.org/ttap/RecordsManagementSystems.pdf.

These publications, which are some of the best in the field, focus on law enforcement systems. If your agency is in the process of establishing or upgrading an RMS, these resources may be quite useful to you.

WHAT EXACTLY IS AN RMS?

A records management system (RMS) is "an agency-wide system that provides for the storage, retrieval, retention, manipulation, archiving, and viewing of information, records, documents, or files pertaining to law enforcement operations. RMS covers the entire life span of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms." (This definition is taken from both the Bureau of Justice Assistance's *Standard Functional Specifications for Law Enforcement Records Management Systems* and the International Association of Chiefs of Police [IACP]/Department of Justices' Community Oriented Policing Services [COPS] Technology Technical Assistance Program's *Records Management Systems* documents.)

"Records" are the information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business. The International Council on Archives (ICA) Committee on Electronic Records defines a record as, "recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity."

For the purpose of this document, records are limited to documents or electronic files directly related to law enforcement operations such as incident and accident reports, arrests, citations, warrants, case management, field contacts, etc., and how these records come into play in the programs and services that the FBI administers.

THE IMPORTANCE OF INCIDENT/OFFENSE REPORTS

(How an RMS can assist agencies in Uniform Crime Reporting [UCR] and the Law Enforcement National Data Exchange [N-DEx] submissions)

The concept of an incident/offense-based reporting system was developed to enhance the capability for capturing accurate information for report writing and recordkeeping activities. An RMS consisting of uniform records such as incident/offense reports is extremely beneficial for law enforcement agencies. For example, an incident/offense-based reporting system satisfies operational and management needs at the local level, as well as the informational requirements of the UCR Program and the recently deployed N-DEx. The incident-based system also assists in identifying reported criminal activity from one area to another.

Such a system provides a uniform incident/offense report that can be incorporated into a law enforcement agency's current records system or easily implemented by an agency that has few if no formalized records. An incident/offense-based reporting system in its simplest form provides a uniform method of preparing, storing, and retrieving information. Disregarding the agency's level of complexity, the system should portray a picture in words and allow for the administrative and management decisions that effectively and efficiently react to the reported criminal activity within that agency's jurisdiction.

What exactly is an incident/offense report?

Typically, an incident/offense report reflects the following information:

- *Persons attacked*: the number of victims; their age, sex, and race; and when possible, their occupations.

- *Property attacked*: the type of premises in which the offense was committed, such as drug store, grocery store, gasoline station, etc. If a building is used for several different purposes, the first purpose for which the particular room entered is used is typically indicated; after that, the general use of the building.

- *How attacked*: the general manner in which the crime was committed. If a burglary occurred, state the location of the door or window by which entrance was gained. In a robbery case, indicate whether the victim was threatened, strong-armed, etc. For a theft, specify the place from which the property was stolen, such as a desk, cash register, car, porch, etc.

- *Means of attack*: any instruments, tools, or devices used in attacking persons or property. In burglary cases, all tools should be specifically described, showing for instance the size of a jimmy or a drill. In robbery cases, the best possible description of the weapons should be given. In theft cases, the means of attack may be the carrying away or driving away of property, shoplifting, etc.

- *Object of attack*: in crimes against property, the property stolen will be the object of attack. The specific type of property, such as money, jewelry, clothing, silverware, etc. should be shown. In crimes against person, the object of attack will be expressed in terms of the motive (as distinguished from any property)—illicit love affair, robbery, quarrel, etc.

- *Trademark*: any peculiarity in the commission of the crime which might aid in distinguishing it from other generally similar crimes.

- *Vehicle used*: as completely as possible, include the year, make, model, color, type, vehicle identification number (VIN), and license plate number of any vehicle used in the commission of a crime.

- *Suspect*: descriptive data of the suspect, such as the age, sex, and race. Also, other descriptive data such as the height, weight, identifiable scars and marks, geographical accents in speech, body odors, or anything which might be helpful in later identifying the suspect is typically included.

LEVELS OF REVIEW

(Keeping middle and upper management informed)

Certain levels of review are suggested to provide the essential involvement of management in report processing. Of course, the number of reviews will depend upon the desire of the particular agency administrator; however, an efficient reporting system provides for three levels of review:

- *By the field supervisor*, who evaluates and approves the work of subordinate officers.

- *By a central records section* who handles the various reporting documents of the agency. From these documents all reports and records of the agency can be generated, e.g., Uniform Crime Reporting (UCR) or the Law Enforcement National Data Exchange (N-DEx) submissions.

- *At the administrative level*, in order for administrators to keep informed and allocate manpower and resources efficiently.

These levels of review are established to ensure the information collected and recorded is adequately analyzed and evaluated. From these levels of review, law enforcement administrators should be able to select the best operational tactics and allocate resources to maximize their agencies' productivity and effectiveness.

First level of review

At the first level of review, the field supervisor should ensure all reports are legible, complete, and accurate. Reports prepared by individual officers should be approved by their immediate supervisors. It is essential that field supervisors understand local ordinances and state and federal statutes, as well as information available and procedures necessary to interact with the National Crime Information Center.

Second level of review

At the second level of review, the Central Records Section should ensure that the report has been approved by a ranking officer and that it is appropriately recorded and filed (whether electronically or manually). If a method compatible with an incident/offense report system is used, data can be extracted at this point for UCR and/or N-DEx submissions and other reports required by the agency.

Third level of review

The third review is at the administrative level. Through this review, reports generated by the agency keep the administration informed so it can allocate manpower and resources most effectively. Typically, the Central Records Section provides summarized, statistical reports, graphs, charts, etc. for administrative use. The administrative level needs instant access through Central Records to provide for adequate responses to the media, city council, requests from judicial agencies, and other legitimate groups.

IDENTIFICATION SYSTEMS AND LAW ENFORCEMENT RECORDS

Integrated Automated Fingerprint Identification System (IAFIS):

Next Generation Identification (NGI)

Interstate Identification Index (III)

What is the IAFIS?

The IAFIS is the national online fingerprint and criminal history database with identification and response capabilities.

The IAFIS consists of five integrated segments:

- The Automated Fingerprint Identification System (AFIS).
- III.
- The Identification Tasking and Networking (ITN).
- The Electronic Fingerprint Converter (EFCON).
- The IAFIS Data Warehouse (IDWH).

The fingerprints are collected and processed at the state level. Upon successful completion at that level, an electronic submission is provided to the IAFIS, which is housed at the FBI's Criminal Justice Information Services (CJIS) Division in Clarksburg, West Virginia. The system through which these transactions occur is comprised of communications equipment, encryption components, and firewalls installed in all 50 states, in U.S. territories, and with other international, federal, tribal, and local criminal and noncriminal justice agency partners that submit fingerprints to the IAFIS. The IAFIS allows the FBI to process hundreds of thousands of tenprint searches per day and also to search latent prints obtained at crime scenes against the master database of known criminal suspects.

Biometric interoperability

Biometric interoperability was initiated in 2005 to facilitate the exchange of information between the Department of Justice (DOJ), the FBI's IAFIS, and the Department of Homeland Security's (DHS's) Automated Biometric Identification System (IDENT). The goal of Biometric Interoperability is to improve information sharing between the FBI's IAFIS and the biometric systems of other federal and international partners.

In September 2006, the FBI, the DHS, and the Department of State (DOS) deployed the Interim Data Sharing Model (iDSM), establishing the platform and processes to share read-only copies of fingerprint images of limited data subsets from the IAFIS and the IDENT in near real-time. The IAFIS subsets include known or suspected terrorists (KSTs) and wanted subjects with an associated FBI record. The IDENT subsets include DHS expedited removals and the DOS category one visa refusals (statutorily inadmissible). Authorized users of each system access the others' records to determine if an encountered subject is located within the shared records, allowing them to make more informed decisions, e.g., admissibility of foreign visitors or visa applicants.

In October 2008, the FBI began transitioning agencies participating in iDSM interoperability to a shared service capability allowing users to submit fingerprints to the IAFIS for a biometric search of the full IDENT repository. Originating agencies now receive criminal history information from the IAFIS and immigration identity information from the IDENT. Participants also receive the immigration status of the individual from the DHS Immigration and Customs Enforcement's (ICE's) Law Enforcement Support Center (LESC). The shared services capability constitutes a major milestone in the information-sharing initiatives between the FBI and the DHS.

As a result of Biometric Interoperability, more state and local law enforcement agencies are gaining biometric-based access to the full IDENT repository through the DHS's ICE Secure Communities Program, which helps identify and remove criminal aliens who pose the greatest threat to local communities. By December 2009, the program was deployed in 102 locations within 13 states. In addition, the IAFIS continues to support additional searches from the DHS and the DOS. By January 2010, the IAFIS supported over 130,000 submissions per day from the DHS and the DOS.

When fingerprints are not available

The CJIS Division will conduct name checks for criminal justice agencies when fingerprints are not available and there is a valid criminal justice need. Records at the CJIS Division relating to persons with dates of birth of 1956 or after are available through the National Crime Information Center's (NCIC's) III. In addition, some records of older persons are also available through the III if their first arrest occurred on or after July 1, 1974. Therefore, criminal justice agencies with access to NCIC terminals should first consider making online inquiries of the III regarding all individuals on whom they would normally mail in name-check requests to the CJIS Division.

Authorized agencies may submit requests to the CJIS Division for name checks on persons with dates of birth of 1955 or earlier who are not in the III. These requests may be sent via mail, e-mail, facsimile, or telephone. A separate request should be submitted for each name. (For more information about the III, see page 13.)

Next Generation Identification (NGI)—the future of identification systems

The industry of identification systems is moving beyond dependency on a unimodal (e.g., fingerprint) biometric identifier and is beginning to incorporate multimodal biometrics (i.e., iris, facial, palm, etc.). In line with this trend, the NGI Program, the future of the FBI's identification systems, will help to foster the framework required for techniques that fuse multimodal biometrics. To accommodate new technologies and emerging biometrics standards, the framework will be expandable and flexible—and will be interoperable with existing systems.

The basic NGI initiatives are Advanced Fingerprint Identification Technology (including Rapid Search Capabilities for the Repository for Individuals of Special Concern [RISC]), Quality Check Automation, Interstate Photo System Enhancements, Disposition Reporting Improvements, Enhanced IAFIS Repository, the FBI National Palm Print System, and an emerging multimodal initiative with potential for an enhanced latent functionality initiative. Once developed and implemented, the NGI initiatives will promote a high level of information sharing, support interoperability, and provide a foundation for using multiple biometrics for positive identification.

Record requirements

The contributors who routinely and voluntarily submit fingerprints and other criminal justice information to the FBI are very important. Their actions expand the size of the fingerprint files, thereby increasing the value of the files to all law enforcement agencies. Mutual cooperation and efficiency are resultant by-products.

The FBI provides all law enforcement agencies access to the FBI's wanted service, as well as its criminal and civil fingerprint files. This timely exchange of information may save an officer's life.

Disposition data and reports

The arrest/booking record of a law enforcement agency is not complete until the final disposition is recorded. Therefore, arrangements should be made to obtain the final disposition for recording on the arrest report in each instance.

To ensure that criminal justice records are as complete as possible, final dispositions for the arrest charges should be furnished to the FBI whenever a fingerprint image has been previously submitted to the Bureau. As the central repository of identification data in the Nation (i.e., the IAFIS, the III/National Fingerprint File [NFF]), the FBI urges each law enforcement agency to follow and report final dispositions. Dismissal and acquittal adjudications are as necessary as conviction information in completing an identification record of an individual. Records must reflect accurately the final results of charges filed alleging violations of the law. It is the incomplete record that invites criticism of the entire criminal justice system. Incomplete records may be subject to purging by court order. Final dispositions should be retained in the case file.

Unfortunately, many agencies continue to afford this vital link in the criminal records system a low priority. As soon as it becomes known, the final disposition data should be reported. Also, the final disposition records should be used to show any change from the original charge as it appears on the arrest fingerprint image to the charge for which conviction was obtained.

Disposition information is also particularly important to the National Instant Criminal Background Check System (NICS), the system that provides authorized law enforcement agencies with information they require to determine whether to allow or deny a firearm transfer.

The final disposition of an arrest is an important addition to an identification record and serves to complete the case history of the offense in the minds of all who later review the record. The FBI number should be placed on the Final Disposition Report when it is known. In the absence of the FBI number, the person's complete name should be reported exactly as it was submitted to the FBI on the fingerprint image. The local arrest number, as shown on the fingerprint image for which the disposition is being submitted, should also be stated on the Final Disposition Report sheet.

Death notices
Statistics on successful identification of the unknown deceased individuals reemphasize the fact that in all cases, fingerprints should be used as the medium for establishing a conclusive and positive identification. If this person's fingerprints are also in FBI files, death notices and/or the fingerprints of the deceased individual should be submitted to the CJIS Division.

Cooperation from local and state law enforcement agencies will make FBI identification records more valuable to all contributors and users and will assist the FBI in providing more prompt, complete, and accurate service to all.

The importance of fingerprinting

Fingerprinting has proven to be a reliable method of identifying individuals. This method is far superior to older methods, such as branding, tattooing, distinctive clothing, photography, and body measurements (Bertillon System). While many cases of mistaken identification have occurred through the use of these older systems, to date the fingerprints of no two individuals have been found to be identical.

There are three basic types of fingerprinting:

- Fingerprinting an individual who is charged with a criminal offense.

- Fingerprinting an applicant as required by local, state, or federal government.

- Fingerprinting for use by agencies when individuals voluntarily desire to submit their fingerprints to the CJIS Division for purposes of personal identification. This type of fingerprinting is also the one used in programs involving the fingerprinting of children initiated pursuant to the Missing Children Act.

Interstate Identification Index (III)/National Fingerprint File (NFF): the decentralized exchange of criminal history records

What is the III/NFF?

The III, a cooperative federal and state effort, enables authorized users to access the Criminal History Record Information (CHRI) for over 63.5 million persons. Approved by the National Crime Information Center (NCIC) Advisory Policy Board (APB) (currently the Criminal Justice Information Services [CJIS] APB) in 1978, the III provides for the decentralized interstate exchange of CHRI and functions as part of the CJIS Division's IAFIS. Currently, 50 states participate in the III Program.

Built upon the foundation of duplicate criminal history repositories and shared record dissemination responsibilities between the III and states' systems, management of the III is shared by the FBI and CJIS Systems Agencies (CSAs) that service III users in their states. All users agree to abide by the rules, policies, and procedures governing III operations. The III provides a means of conducting national criminal history record searches for criminal justice and other purposes as specified by existing local, state, and/or federal laws. The III System processes more than 10 million name-based inquiries each month to determine whether a matching index record is on file. If a match is found, an authorized agency may request the subject's record by transmitting a second inquiry using a unique FBI or State Identification Number assigned to the subject's record. This information is invaluable to investigators, prosecutors, courts, and other III users.

When the III concept was adopted to decentralize criminal history record keeping in 1978, the NFF was the concept's ultimate goal. When fully implemented, the NFF will be a decentralized system that will replace the FBI's record keeping responsibility for state offenders by making state repositories primarily responsible for record dissemination and maintenance. An NFF state submits a single fingerprint image for each offender to the FBI to identify the offender at the national level. Arrest fingerprint images and related disposition and expungement documents for subsequent arrests are used by the state to update its own records; only those fingerprint images that a state is unable to identify will be forwarded to the FBI. Accordingly, state repositories will become the only sources of state criminal history records for these arrests, for both criminal and noncriminal justice purposes.

THE NATIONAL CRIME INFORMATION CENTER (NCIC) AND LAW ENFORCEMENT RECORDS

There is an important relationship between law enforcement records and the NCIC. Local, state, and federal law enforcement agencies depend on the NCIC to provide accurate information in support of their mission to enforce laws and protect the public. However, without recording information properly, the input would be inaccurate, and consequently, the NCIC System would be ineffective.

What is the NCIC?

The NCIC is a nationwide, computerized information system established as a service to all criminal justice agencies—local, state, and federal. The goal of the NCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information.

The NCIC operates under a shared management concept between the FBI and state and federal criminal justice agencies. The FBI maintains the host computer while providing a telecommunication network to the CJIS System Agency (CSA) in each of the 50 states, the District of Columbia, Puerto Rico, the U.S. Virgin Islands, Guam, and Canada, as well as federal criminal justice agencies. These CSAs are the criminal justice agencies that have overall responsibility for the administration and usage of the NCIC within a district, state, territory, or federal agency. These agencies generally operate their own computer systems, providing NCIC access to virtually all local criminal justice agencies. Through this cooperative network, law enforcement personnel have direct on-line access to enter or search millions of records for persons or property. Agencies that enter records in the NCIC are responsible for their accuracy, timeliness, and completeness.

Records

The NCIC database consists of 19 files, the information for which is provided by law enforcement and criminal justice agencies that use the system in the course of their work. There are 7 property files and 12 person files.

The 7 property files, the year the files became part of the NCIC System, and the type of information/records that the files contain are listed below.

- **Article File** (1967)—Records for any item valued at $500 or more; records for all property taken, regardless of value, if the aggregate value taken in one theft exceeds $5,000; records for property taken, regardless of value, if the investigation indicates interstate movement of the property; or records for property taken in which the seriousness of the crime indicates that the investigating agency should enter a record for investigative purposes.
- **Boat File** (1969)—Records for stolen boats.
- **Gun File** (1967)—Records for stolen weapons; recovered (abandoned, seized, or found) weapons; lost or missing weapons; or weapons that have been used in the commission of a felony.

- **License Plate File** (1967)—Records for stolen license plates.
- **Securities File** (1968)—Records for securities that were stolen, embezzled, used for ransom, or counterfeited. Securities are identified as currency and documents or certificates that are evidence of debt or ownership of property or documents that represent subscription rights. Examples of securities include Federal Reserve notes, warehouse receipts, traveler's checks, money orders, stocks, and bonds.
- **Vehicle File** (1967)—Records for stolen vehicles, vehicles used in the commission of a felony, or vehicles that a law enforcement agency may seize based on a federally issued court order.
- **Vehicle/Boat Part File** (1999)—Records for component parts stolen from a vehicle or boat.

The 12 person files, the year the files became part of the NCIC System, and the type of information/records that the files contain are listed below.

- **Convicted Sexual Offender Registry File** (1999)—Records for persons who have been convicted for a criminal offense against a minor, or for a sexually violent offense or for persons whom authorities determined are sexually violent predators are contained within this file.
- **Foreign Fugitive File** (1987)—Only the International Criminal Police Organization (INTERPOL) and the Royal Canadian Mounted Police (RCMP) may enter records into this file. The INTERPOL's records contain information on persons wanted in other countries for crimes that would be felonies if committed in the United States. The wanting country must have signed an extradition treaty or convention with the United States. The RCMP's records contain information on persons who are wanted for violations of the Criminal Code of Canada and for whom there is an outstanding Canada-wide warrant.
- **Identity Theft File** (2005)—Records for victims of identity theft with descriptive and other information that law enforcement personnel can use to determine if an individual is a victim of identity theft or if the individual may be using a false identity.
- **Immigration Violator File** (1996)—Only the Department of Homeland Security's Bureau of Immigration and Customs Enforcement may enter records into this file, which contains records for criminal aliens whom immigration authorities deported for drug or firearms trafficking, serious violent crimes, or both. The file contains information on aliens who have outstanding administrative warrants for removal from and who have unlawfully remained in the United States. The file also contains records for aliens who have outstanding administrative warrants for failure to comply with national security registration requirements.
- **Missing Person File** (1975)—Records for missing persons of any age who have a proven physical or mental disability, records for persons who are missing under circumstances indicating that they may be in physical danger or abducted, records for persons missing after a catastrophe, records for persons under the age of 21 who do not meet any of the above criteria, and records for persons aged 21 and older who are missing that do not meet any of the above criteria but for whom there is a reasonable concern for their safety.

- **Protection Order File** (1997)—Records for individuals who are subject to court-issued orders to prevent violent or threatening acts, harassment against, contact or communication with, or physical proximity to another person.
- **Supervised Release File** (1999)—Records for individuals who are under specific restrictions during their probation, parole, supervised release, or pre-trial sentencing periods.
- **Unidentified Person File** (1983)—Records for unidentified deceased persons, living persons who are unable to verify their identities, unidentified catastrophe victims, and recovered body parts.
- **U.S. Secret Service Protective File** (1983)—Only the U.S. Secret Service may enter records into this file, which contains records for individuals whom the U.S. Secret Service determines to pose a potential threat to the President and other persons protected by the U.S. Secret Service.
- **Gang File** (2009)—Records for violent gangs and their members. *This file was originally part of the Violent Gang and Terrorist Organization (VGTOF) File created in 1995.*
- **Known or Appropriately Suspected Terrorist File** (2009)—Records for terrorist organizations and their members. *This file was originally part of the VGTOF File created in 1995.*
- **Wanted Person File** (1967)—Records for individuals who have an outstanding warrant. This file also contains records for juveniles who have been judged delinquent and who have escaped from custody or supervision or who have absconded while on probation or parole. The file also contains records for juveniles who were charged with committing an act of delinquency that would be a crime if committed by an adult and who have fled from the state in which the act was committed. Agencies may also enter temporary felony want records into this file. Temporary felony want records allow a law enforcement agency to take prompt action to apprehend a person suspected of committing a felony when circumstances prevent the agency from immediately obtaining a warrant.

Other associated files

- **Image File** (1999)—Images can be associated with NCIC records to assist agencies in identifying people and property items. In addition to identifying images, the file contains generic images that can be used as references for particular makes and models of vehicles and boats.
- **Interstate Identification Index (III)** (1983)—The III is not an NCIC file but is an index accessible through the NCIC System. The III contains personal descriptor information that an authorized agency can use to determine if a subject has a state or federal criminal history record on file. A positive response from the III will include instructions on how the agency can retrieve the corresponding history record.
- **Originating Agency Identifier (ORI) File** (1985)—Agencies must have an ORI in order to access the NCIC System. The ORI File contains contact information (such as an agency's address and telephone number) for agencies that have an ORI.

More about the NCIC

The idea of NCIC was conceived in the early 1960s, when it appeared that advances in computer technology could answer law enforcement's growing need for timely, vital information. The FBI, in conjunction with the Advisory Group to the Committee on Uniform Crime Records and the International Association of Chiefs of Police (IACP), recognized the advantages a computerized index of information could offer criminal justice agencies. It became operational in January 1967.

THE LAW ENFORCEMENT NATIONAL DATA EXCHANGE (N-DEx) AND LAW ENFORCEMENT RECORDS

What is the N-DEx?

The N-DEx is a national system designed to search, link, analyze, and share criminal justice information (e.g., incident and case reports) currently housed in various information systems and recorded in a number of formats across the country. More specifically, the N-DEx allows participating law enforcement agencies to detect relationships between people, places, things, and crime characteristics by "connecting the dots" between data that on the surface do not appear to be related. In addition, it provides contact information and collaboration tools for law enforcement agencies that are working on cases of mutual interest. This new investigative tool primarily benefits local law enforcement in its role as the first line of defense against crime and terrorism.

The N-DEx has been developed and deployed incrementally. Increment 1 became available in March 2008 and provides law enforcement agencies with the ability to search the N-DEx based on people, vehicles/property, location, and/or crime characteristics, and supports multi-jurisdictional task forces. Increment 2 was deployed in July 2009 and provides additional functions such as automated processing, collaboration, subscription, and notification (including incarceration and booking data). The N-DEx interfaces with and queries the National Crime Information Center (NCIC) and the Interstate Identification Index (III).

Law enforcement agencies are the primary users of the system, and expansions of the system are incorporating the full criminal justice community. The ultimate goal is to transform all criminal justice data into knowledge for the entire justice community while maintaining privacy and security. The life-cycle participants include corrections and probation/parole agencies.

The N-DEx offers a range of options to allow broad-based participation. Agencies using fully automated RMSs can benefit from the N-DEx as well as those agencies having paper-based systems.

What the N-DEx is NOT

The N-DEx is not a statistical reporting system

The N-DEx is an information-sharing system and is not intended to be used for reporting crime statistics, a function that is provided by the Uniform Crime Reporting (UCR) Program. The N-DEx and the UCR Program are separate programs. A law enforcement agency may report the UCR Program's National Incident-Based Report System (NIBRS) data through the N-DEx if it so chooses; however, an agency does not have to change its current method of UCR/NIBRS reporting to participate in the N-DEx.

The N-DEx is not an intelligence system, but it has intelligence value

The N-DEx is not an intelligence system and does not contain intelligence data. However, similar to other criminal justice systems (the NCIC, et al.), the N-DEx System's information and tools will provide value to the intelligence community.

Data sources

The N-DEx seeks to use existing systems and networks

Many potential N-DEx participants are already members of another trusted information-sharing community (state, regional, federal, etc.). These users usually access and provide information through local mechanisms and sanctioned business processes. The N-DEx provides well-defined integration points allowing for inclusion of existing groups, technologies, and locally vetted identities and policies into its broader information-sharing architecture (i.e., the Criminal Justice Information Services (CJIS) systems, OneDOJ, other DOJ components, and other federal law enforcement agencies).

Role of the CJIS Systems Officers (CSOs) in the N-DEx

The FBI's CJIS Division has worked closely with state CSOs in the development and implementation of many of the CJIS systems that are replicated or that provide service to local, state, tribal, and federal law enforcement agencies. This approach creates a central (single) point of contact (POC) for many CJIS-related matters, including the responsibility/accountability for access and use of CJIS systems. Working with CSOs also helps close the gap in laws and statutes relative to the operation of these systems as well as the varied types of systems that connect and interact with them. Because of this varied landscape, the preferred method for N-DEx connectivity with systems that will provide data to the N-DEx is through this central CSO point within each of the 50 states. However, this may not be feasible in the short term, as the capabilities of many state CSOs are also varied; many are not ready to receive or transport data to the N-DEx. Because of the variations among the systems and RMSs within law enforcement agencies nationally, the N-DEx Program may be required to accept data or interface with user systems under a wider (less centralized) approach, which would also include Fusion Centers and regional information-sharing efforts that fall outside of the auspices of the CSOs. Connectivity with any of the various systems will need to be coordinated through the CSOs to ensure compliance with applicable local and state laws and regulations.

Records

All information shared through the N-DEx originates from data supplied by the participating local, state, tribal, and federal systems, which include, but are not limited to:

- Incident reports
- Arrest reports
- Case files
- Booking reports
- Incarceration records
- Criminal histories
- Probation/parole reports

These records contain information about entities (e.g., people, locations, and items such as weapons and vehicles) and may specify relationships among the entities they contain (e.g., the individual's residential address or vehicle description).

The N-DEx transforms raw contributor data into information that can be easily shared, searched, and queried to support investigations and analyses, including entity and relationship, incident/case correlation, geospatial products, and automated processing.

Ownership of data shared in the N-DEx remains with the agency that provided it. The originating agency controls what data to share, who can access it, and under what circumstances the data can be accessed. It allows agencies to participate in accordance with applicable laws and policies governing dissemination and privacy.

More about the N-DEx

Data standards

The developers of the N-DEx look to data standards that are already in existence and widely accepted. These standards include the work of Global, the Global Justice Extensible Mark-Up Language Data Model (GJXDM), the National Information Exchange Model (NIEM), and the Law Enforcement Information Sharing Program (LEISP) Logical Entity Exchange Specification (LEXS) based on the latest NIEM release, et al.

Organizational accountability

An essential element for successful interagency cooperation is organizational accountability. A Memorandum of Understanding (MOU)/User Agreement is the means by which the N-DEx documents what has been agreed upon with its information-sharing partners, including standards and controls that address access to each partner's data. A standard MOU/User Agreement is employed but is augmented to address unique relationships with data providers.

Classification

Only data categorized as Controlled Unclassified Information (CUI) or below are permitted within the N-DEx.

THE NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM (NICS) AND LAW ENFORCEMENT RECORDS

What is the NICS?

The NICS is a national background check system that checks all available records to determine if an individual is eligible to receive and/or possess firearms. The NICS was created as a result of the Brady Handgun Violence Prevention Act (Brady Act) of 1993, Public Law 103-159. The FBI developed the NICS through a cooperative effort with the Department of Justice; the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and state and local law enforcement agencies. The FBI maintains and facilitates the NICS while the ATF enforces the parameters of the law. In the majority of cases, the results of background check inquiries provide definitive information on the subject's eligibility within 30 seconds of the data entry of an individual's descriptive information into the NICS. Some states conduct their own background checks by designating a state or local law enforcement authority within the state to serve as an intermediary between the Federal Firearms Licensees (FFLs) and the NICS in a point of contact (POC) capacity. The FFLs contact either the FBI or a designated state POC to initiate background checks on individuals attempting to purchase or redeem firearms, and in certain instances, obtain firearm-related permits.

POC states

In states that agree to serve as POCs for the NICS, the functions performed by the CJIS Division's NICS Section are performed by state or local law enforcement agencies which service the FFLs. The FFLs contact these state or local agencies which perform the background checks, make final status decisions, and notify the FFL of the results of the check. There are three methods of initiating background checks, depending upon the state in which the FFL is conducting business:

1. POC States: In states that have agreed to serve as the POC for the NICS, the FFLs contact the NICS through the state POC for all firearm transfers. The state POC conducts the NICS check and determines whether the transfer would violate federal or state law.

2. Non-POC States: In states that have declined to serve as the POC, the FFLs initiate a NICS background check by contacting the NICS Section for all firearm transfers. The FBI conducts the NICS check and determines whether the transfer would violate federal or state law.

3. Partial-POC States: In states that have agreed to serve as a partial-POC for handgun transfers but not for long gun transfers, the FFLs contact the NICS through the designated state POC for handgun transfers and the NICS Section for long gun transfers.

Brady Act requirements

The NICS was mandated by the Brady Act and was established for FFLs to contact by telephone or other electronic means for information to be supplied immediately on whether the transfer of a firearm would violate Section 922 (g) or (n) of Title 18, United States Code, or state law. FFLs must be a licensed dealer through the ATF and be enrolled with the FBI to initiate background checks with the NICS. The NICS background checks are required for the transfer or redemption of firearms, including both handguns and long guns.

Persons holding firearm permits which qualify as alternates to a NICS check, per the ATF, are not required to undergo a NICS check at the time of transfer. During the alternate permit-issuing process, a NICS check is conducted. The former pawnshop exemption for background checks on individuals redeeming firearms ceased to exist on November 30, 1998.

The Safe Explosives Act was enacted on February 25, 2002, as part of the Homeland Security Act and required that any person who transports, ships, causes to be transported, or receives explosives materials in either interstate or intrastate commerce must obtain a federal permit or license issued by the ATF after undergoing a background check. In February 2003, the transfer of explosives was added to the NICS background check requirements.

Record requirements

The NICS researches and evaluates criminal history and other record information (e.g., domestic violence records, mental health records, etc.) returned in response to firearm background check inquiries resulting in a delay status to determine an individual's eligibility to receive firearms and/or permits pursuant to the Brady Act. The NICS responds to customers, FFLs, the general public, etc., on information as it relates to the Brady Law and makes referrals to the ATF. The NICS Section staff also research and evaluate disposition information requested from local, state, and federal criminal justice and law enforcement agencies. The NICS ensures compliance regarding the safeguarding of privileged personal data when providing information to entities outside of the NICS Section concerning transaction notification and information-sharing processes. In addition, it advises local, state, and federal criminal justice agencies regarding the location of fugitives/individuals on probation and parole who are attempting to purchase a firearm. The NICS Section also is instrumental in effecting the update of applicable federal, state, and local automated criminal history databases to ensure the availability of current record information for future inquiries by law enforcement agencies. Concurrent with the NICS Section's firearms responsibilities, NICS staff research and evaluate state and/or federal laws as they apply to firearms and legal processes (e.g., restoration of rights, protection order criteria, etc.).

The absence of complete disposition information is a common reason why responses are delayed. In such instances, the NICS Section staff typically must contact a state or local entity, usually a court, to determine an individual's eligibility to purchase or possess a firearm. Based on federal law, an arrest alone cannot preclude an individual the transfer of a firearm. The NICS Section may also need to verify indictments, the results of drug tests, or obtain filed information to determine if an individual is prohibited from purchasing or possessing firearms. If complete information cannot be obtained within the mandated 3-business-day limit, it is at the discretion of the FFL whether to allow the firearm transfer. However, the NICS Section staff continue to research the transaction for up to 88 days in an effort to obtain complete disposition information.

Information that is NOT retained

The NICS does not establish or create a federal firearm registry. Pursuant to Title 28, Code of Federal Regulations (C.F.R.), Section 25.9 (b) (1), the NICS is required to destroy all personally identifying information (other than the identifying transaction number and the date the number was assigned) submitted by or on behalf of any person who has been determined not to be prohibited from possessing or receiving a firearm no more than 24 hours after the FFL has been notified of the proceed decision. Pursuant to NICS Regulations, 28 C.F.R. §25.2, the NICS can retain records of delayed (open status) transactions until either (1) a final determination on the transaction is reached and has been communicated to the FFL resulting in the status being changed to a "proceed" (records purged within 24 hours) or a "denied" (records retained indefinitely) status, or (2) 90 days elapse from the date of inquiry. If no additional information is obtained to make a final determination of "proceed" or "deny" on the transaction, all identifying information (with the exception of the NTN and creation date) is purged by the NICS 88 days from the creation date.

How the NICS process works

As a result of the Brady Act, all individuals attempting to purchase a firearm from an FFL are required by law to have a NICS check performed prior to obtaining a firearm. When purchasing a firearm, the individual is required to complete and sign the ATF Form 4473 with descriptive information such as name, sex, race, date of birth, and state of residence along with other information. Upon completion, the FFL provides the NICS with the necessary data from the ATF Form 4473 to initiate a background check. Once the information is received, a name and limited descriptor search is conducted for matching records in the Interstate Identification Index (III), which contains millions of criminal history records; the National Crime Information Center (NCIC), which contains documented criminal justice information such as arrest warrants, protection orders, etc.; and the NICS Index, which contains information not maintained in the III or the NCIC contributed by federal, state, local, and tribal agencies pertaining to persons federally prohibited from receiving or possessing firearms. Information in the NICS Index includes (but is not limited to) protection orders and active warrants not located in the NCIC; persons who are under a court order not to possess a firearm; a felony conviction posted to a state record not reflected in the III; records exhibiting an illegal/unlawful alien status; and/or individuals meeting the federally established criteria pertaining to mental health/illness. In addition, if the individual is a non-U.S. citizen, the databases of the Department of Homeland Security's U.S. Immigration and Customs Enforcement, more commonly referred to as the ICE, are also queried to determine if the individual is legally and lawfully in the United States and can lawfully receive/possess a firearm.

If no matching records are returned by any of the databases, the transaction is automatically "proceeded," which means the firearm transfer can occur. If the NICS returns a match of the prospective firearm transferee's descriptive information to information in any of the databases, the FFL is advised the transaction is "delayed." In these cases, the FFL is transferred to the NICS Section for review by a Legal Instruments Examiner (NICS Examiner) while still on the telephone. During this process, the NICS Examiner will review information returned by the databases to determine if federal or state firearm prohibitive criteria exist. If the information matched by the NICS is not a valid match or no prohibitive criteria exist, the NICS Examiner advises the FFL they can proceed with the firearm transfer. The FFL must record the NICS Transaction Number (NTN) assigned to the transaction on the ATF Form 4473 and retain the form for auditing purposes.

If it is determined prohibitive criteria exist, the NICS Examiner advises the FFL to deny the firearm transfer. If potentially prohibitive criteria exist and more information is required in order to make a determination, the NICS Examiner will advise the FFL to "delay" the firearm transfer. When a transfer is delayed, the NICS Examiner begins extensive research on the potential prohibitor(s).

The Brady Act provides 3 business days for the purpose of obtaining additional clarifying information to make a determination as to the prospective transferee's eligibility. Some inquiries may take longer than 3 business days to obtain relevant information to make a decision on whether the transfer of the firearm may proceed or be denied. The NICS Section employees also research and evaluate disposition information returned from federal, state, local, and tribal criminal justice and law enforcement agencies. During this exchange of information, the NICS Section ensures compliance regarding the safeguarding of privileged personal data when providing information to external entities concerning transaction notification and information-sharing processes. In addition, the NICS Section advises federal, state, and local law enforcement agencies regarding the location of fugitives who are attempting to purchase a firearm. After gathering information from the background check process, the NICS Section attempts to update applicable federal, state, local, and tribal automated criminal history information to ensure the availability of current and complete record information for future inquiries by law enforcement agencies.

Ten federal firearms prohibitions that prevent a person from receiving firearms or explosives:

1. A person who has been convicted in any court of a crime punishable by imprisonment for a term exceeding 1 year or any state offense classified by the state as a misdemeanor and is punishable by a term of imprisonment of more than 2 years.

2. Persons who are fugitives from justice; for example, the subject of an active criminal warrant.

3. An unlawful user and/or an addict of any controlled substance. For example, a person convicted for the use or possession of a controlled substance within the past year, or a person with multiple arrests for the use or possession of a controlled substance within the past 5 years with the most recent arrest occurring within the past year, or a person found through a drug test to use a controlled substance unlawfully, provided the test was administered within the past year.

4. A person adjudicated mental defective or involuntarily committed to a mental institution or incompetent to handle their own affairs, including being found not guilty by reason of insanity or found incompetent to stand trial for criminal charges.

5. A person who, being an alien, is illegally or unlawfully in the United States. A person who, being an alien except as provided in 18 U.S.C. § 922 (y) (2), has been admitted to the United States under a non-immigrant visa.

6. A person dishonorably discharged from the United States Armed Forces.

7. A person who has renounced their United States citizenship.

8. A person who is the subject of a court order issued after a hearing in which the respondent had notice that restrains them from harassing, stalking, or threatening an intimate partner or child of such partner. This does not include ex parte orders.

9. A person convicted in any court of a misdemeanor crime which includes the use or attempted use of physical force or threatened use of a deadly weapon and the defendant was the spouse, former spouse, parent, guardian of the victim, by a person with whom the victim shares a child in common, by a person who is cohabiting with or has cohabited in the past with the victim as a spouse, parent, guardian or similarly situated to a spouse, parent, or guardian of the victim.

10. Persons who are under indictment or information for a crime punishable by imprisonment for a term exceeding 1 year.

NICS E-Check

The NICS E-Check enables the FFLs to initiate an unassisted NICS background check for firearm transfers via the Internet during the hours of 8 a.m. to 1 a.m., 7 days a week (Eastern time). FFLs have the capability to retrieve results of background checks 24/7. FFLs who are registered to use the NICS E-Check have the flexibility of using the telephone or Internet, in any combination, to initiate and determine final statuses of NICS checks. The NICS E-Check is monitored for misuse and unauthorized access and denies access to any individual whose identification is not known to the system.

NICS Appeals

Individuals who are denied the purchase of a firearm may request the NICS Section or the state which processed their NICS check to provide the reasons for the denials. The provisions for appeals are outlined in subsection 103 (f) and (g) and Section 104 of the Brady Act and also in the NICS Regulations, 28, C.F.R., §25.10. Appeals may be submitted via facsimile to 1-888-550-6427 or 1-304-625-0535; by e-mail at <nicsappeals@leo.gov>; or by mail to the NICS Section, Appeal Services Team, Post Office Box 4278, Clarksburg, West Virginia, 26302-9922. Appellants must include the NTN assigned to their transaction along with their complete mailing address when requesting an appeal.

NICS Voluntary Appeal File (VAF)

Pursuant to 28 C.F.R., Part 25.9 (b) (1), all identifying information associated with approved firearm transfers is destroyed within 24 hours of the FFL being notified of the proceed status. The destruction of such information does not allow the NICS to maintain specific and readily available record-clarifying or record-nullifying information that could assist the NICS with determining an individual's eligibility to receive or possess firearms. The VAF is a computer-based file that houses information/documentation, voluntarily provided, about eligible purchasers to assist the NICS in justifying the individual's firearms eligibility status during the background check process. The VAF permits lawful purchasers who have experienced delays or erroneous denials for a firearm transfer to request the NICS Section maintain information about them in a separate file to be accessed during a NICS check to prevent delays and erroneous denials in the future. When an applicant is approved for entry into the VAF, a unique personal identification number (UPIN) is assigned and should be provided to the FFL during subsequent background checks. The presentation of an active UPIN prompts the review of additional information maintained in the VAF in support of an accurate and timely background check determination. The NICS Section is required to destroy any records submitted to the VAF upon written request from the individual.

Privacy and security of NICS information

The privacy and security of the information in the NICS is strictly mandated by the Brady Act. In October 1998, the U.S. Attorney General published regulations on the privacy and security of NICS information, including the proper and official use of this information. Data stored in the NICS is documented federal data, and access to that information is restricted to agencies authorized by the FBI. Extensive measures are taken to ensure the security and integrity of the system information and agency use. To ensure the integrity of the NICS and identify instances of misuse, audits of those entities and individuals who have access to the system are conducted by the FBI. In addition, the FBI performs audits of the NICS records in accordance with the NICS Regulations to ensure compliancy.

THE UNIFORM CRIME REPORTING (UCR) PROGRAM AND LAW ENFORCEMENT RECORDS

The Summary Reporting System

The National Incident-Based Reporting System (NIBRS)

Law Enforcement Officers Killed and Assaulted (LEOKA) Program

Hate Crime Statistics Program

What is the UCR Program?

The FBI's UCR Program is a nationwide, cooperative statistical effort of more than 17,000 city, university and college, county, state, tribal, and federal law enforcement agencies voluntarily reporting data on crimes brought to their attention. Since 1930, the FBI has administered the UCR Program and continues to collect and publish crime statistics that provide a picture of the nature and type of crime in the Nation. The program's primary objective is to generate reliable information for use in law enforcement administration, operation, training, and management; however, its data have over the years become one of the country's leading social indicators. Criminologists, sociologists, legislators, municipal planners, the media, and other students of criminal justice use the data for varied research and planning purposes.

The UCR Program's annual report, *Crime in the United* States, and the raw data collected by the program, which are also made available by the FBI, provides a picture of the nature and scope of crime in the Nation. In addition to crime statistics, the UCR Program also collects and publishes information about the officers who are killed, feloniously or accidentally, and those who are assaulted in the line of duty and information about crimes that are motivated by prejudice based on race, religion, sexual orientation, ethnicity/national origin, or disability. These data are published in the program's annual reports *Law Enforcement Officers Killed and Assaulted* and *Hate Crime Statistics*, respectively.

Record requirements

There is a close relationship between law enforcement records and the preparation of the UCR Program's reports as nationwide law enforcement statistics must necessarily depend upon information from the records of local agencies. A good records system is an essential base for accurate crime reporting. If properly prepared, the Uniform Crime Reports can become a valuable tool for management purposes within the agency.

Summary Reporting System

Law enforcement agencies (e.g., police, sheriffs, and state police) report the number of offenses that are known to them on a monthly basis in the Part I crime categories (murder and nonnegligent manslaughter, forcible rape, robbery, aggravated assault, burglary, larceny-theft, motor vehicle theft, and arson) and Part II crime categories (all other crimes except traffic offenses). Only information concerning persons arrested is collected for the Part II crimes. (More details about these offenses can be found in the *Uniform Crime Reporting Handbook*.)

To provide for nationwide uniformity in the reporting of Part I and Part II offenses, standardized definitions were adopted. This standardization was created to ensure that the uniform classification overcomes the variations in definitions of criminal offenses in states and localities throughout the country. Reporting agencies are required to interpret local criminal offenses in the context of these definitions prior to submitting their crime counts to the FBI. By doing so, participating law enforcement agencies provide the national UCR Program with regular crime data which allow for a periodic, nationwide assessment of crime not available elsewhere in the criminal justice system.

The NIBRS

The NIBRS is an incident-based reporting system, which means data are collected on each single crime occurrence. The NIBRS includes data on each single incident and arrests within 22 offense categories and is made of 46 specific crimes called Group A offenses and 11 Group B offense categories for which only arrest data are collected. (Complete details of the NIBRS are provided in the *Uniform Crime Reporting Handbook, NIBRS Edition*.)

Originally designed with 52 data elements, the NIBRS captures up to 57 data elements via six types of data segments: administrative, offense, victim, property, offender, and arrestee. Four modifications have been made to the system: To meet growing challenges in the fight against crime, the system's flexibility has permitted the addition of a data element to capture bias-motivated offenses (1990), the expansion of an existing data element to indicate the presence of gang activity (1997), the addition of three data elements to collect data for law enforcement officers killed and assaulted (2003), and the addition of a data element to collect cargo theft offenses (2010).

The FBI began accepting NIBRS data from a handful of agencies in 1989. Twenty years later, most states are now certified to report crime data via the NIBRS.

Requirements for NIBRS participation

Since data collected by the NIBRS are considerably more comprehensive than those of the traditional Summary Reporting System, agencies wishing to participate must have computerized data systems capable of processing NIBRS information. The NIBRS was designed to be a byproduct of an existing automated law enforcement records system.

Full participation in the NIBRS necessitates meeting all the reporting guidelines/requirements set forth in the *Uniform Crime Reporting Handbook, NIBRS Edition*. There is a lower level of participation, which may be allowed if a state or local agency is unable to meet all of the offense-reporting requirements of full participation. Under limited participation, detailed incident reporting is reduced from 22 NIBRS Group A offense categories to the Part I offenses, including the expanded Forcible Sex Offenses. Other offenses are to be reported only when arrests occur. All of the other requirements for NIBRS participation must be met.

Additional information about the compatibility of law enforcement RMSs to the NIBRS is provided in the FBI's *Handbook for Acquiring an RMS that is compatible with the NIBRS*.

Record standards for the Summary Reporting System and the NIBRS
The following standards in records and reports are necessary for any agency which expects to generate Uniform Crime Reports from its records system:

1. A permanent record of each crime is made immediately upon receipt of the complaint. All reports of thefts or attempted thefts are included regardless of the value of property involved.

2. Staff or headquarters' control exists over the receipt of calls for service to ensure that each is promptly recorded and accurately tabulated.

3. An investigative report is made in each case showing fully the details of the offense as alleged by the complainant and as disclosed by the investigation. An effective follow-up system is used to see that reports are promptly submitted in all cases.

4. All reports are checked to see that the crime classifications conform to the uniform classification of offenses. That is, all offenses reported to the UCR Program, regardless of what the offense is called at the local or state level, should conform to the UCR Program's classification of offenses.

5. The offense reports on crimes cleared by arrest or exceptional means are noted as cleared.

6. Arrest records are complete, special care being taken to show the final disposition of the charge.

7. Records are centralized; records and statistical reports are closely supervised by the administrator; periodic inspections are made to see that the rules and regulations of the local agency relative to records and reports are strictly followed.

8. Statistical reports conform in all respects to the UCR Program's standards and regulations.

More about the UCR Program

Recognizing a need for national crime statistics, the IACP formed the Committee on Uniform Crime Records in the 1920s to develop a system of uniform crime statistics. After studying state criminal codes and making an evaluation of the recordkeeping practices in use, the Committee completed a plan for crime reporting that became the foundation of the UCR Program in 1929. The plan included standardized offense definitions for the seven main offense classifications (Part I crimes) to gauge fluctuations in the overall volume and rate of crime. By congressional mandate, arson was added as the eighth Part I offense category in 1979. Developers also instituted the Hierarchy Rule as the main reporting procedure for what is now known as the Summary Reporting System of the UCR Program.

In January 1930, 400 cities representing 20 million inhabitants in 43 states began participating in the UCR Program. Congress enacted Title 28, Section 534, of the United States Code authorizing the Attorney General to gather crime information that same year. The Attorney General, in turn, designated the FBI to serve as the national clearinghouse for the crime data collected. Every year since, data based on uniform classifications and procedures for reporting offenses and arrests have been obtained from the Nation's law enforcement agencies.

Although the data collected and disseminated by the UCR Program remained virtually unchanged throughout the years, in the 1980s a broad utility had evolved for UCR. Recognizing the need for improved statistics, law enforcement called for a thorough evaluative study to modernize the UCR Program. The FBI concurred with the need for an updated program and lent its complete support, formulating a comprehensive three-phase redesign effort. With the three phases completed (including a pilot demonstration that ran from March 1 through September 30, 1987), the FBI held a National UCR Conference on March 1–3, 1988, to present the redesigned system to law enforcement and to obtain feedback on its acceptability. Attendees of the National UCR Conference passed three overall recommendations without dissent: first, that there be established a new, incident-based national crime reporting system (which, when developed and implemented, became the NIBRS); second, that the FBI manage this program; and third, that an Advisory Policy Board composed of law enforcement executives be formed to assist in directing and implementing the new program. Furthermore, attendees recommended that the implementation of national incident-based reporting proceed at a pace commensurate with the resources and limitations of contributing law enforcement agencies.

From March 1988 through January 1989, the FBI proceeded in developing and assuming management of the UCR Program's NIBRS, and by April 1989, the national UCR Program received the first test submission of NIBRS data. In 2009, most states are certified to report crime data via the NIBRS. (More details about the NIBRS can be found in the *Uniform Crime Reporting Handbook, NIBRS Edition*.)

The UCR Program's LEOKA data collection

The FBI publishes *Law Enforcement Officers Killed and Assaulted* each year to provide information about the officers who were killed, feloniously or accidentally, and those officers who were assaulted while performing their duties. The FBI collects these data through the UCR Program.

The UCR Program collects information monthly about assaults on duly sworn city, university and college, county, state, and tribal law enforcement officers. The agencies that employ these officers collect and submit data either through their state UCR Programs, or, for non-program states, directly to the FBI.

When an officer is killed in the line of duty, the FBI gathers data about circumstances pertaining to the death. The data come from various sources:

- City, university and college, county, state, tribal, and federal law enforcement agencies participating in the UCR Program may report line-of-duty deaths that occur in their jurisdictions.
- FBI field divisions report line-of-duty deaths of United States law enforcement officers that occur in the United States and its outlying areas.
- Several nonprofit organizations, such as the Concerns of Police Survivors and the National Law Enforcement Officer's Memorial Fund, which provide various services to the families of fallen officers, also provide information about line-of-duty deaths.

When the FBI receives notification of a line-of-duty death, the LEOKA staff works with FBI field offices to contact the fallen officer's employing agency, requesting additional details about the fatal incident and supplying information about federal programs that provide benefits to survivors of law enforcement officers killed in the line of duty. The LEOKA staff also obtains criminal history data from the FBI's III about people who are identified in connection with line-of-duty felonious deaths.

Federal officers

Data published by the FBI concerning federal officers who were killed or assaulted in the line of duty are provided by the following six federal agencies:

- U.S. Capitol Police
- U.S. Department of Homeland Security
- U.S. Department of the Interior
- U.S. Department of Justice
- U.S. Department of the Treasury
- U.S. Postal Inspection Service

Within these departments are the agencies, bureaus, and services that employ most of the personnel who are responsible for protecting government officials and enforcing and investigating violations of federal law. Every year, the FBI contacts these agencies and requests information about the officers who were killed or assaulted in the line of duty.

The information concerning federal officers differs slightly from the data regarding assaults on city, university and college, county, state, and tribal law enforcement officers. First, the data regarding federal officers include all reports of assaults regardless of the extent (or the absence) of personal injury. Second, the circumstance categories are tailored to represent the unique duties of federal law enforcement personnel.

More about the LEOKA Program

Beginning in 1937, the FBI's UCR Program collected and published statistics on law enforcement officers killed in the line of duty in its annual publication, *Crime in the United States*. Statistics regarding assaults on officers were added in 1960. In June 1971, executives from the law enforcement conference, "Prevention of Police Killings," called for an increase in the FBI's involvement in preventing and investigating officers' deaths. In response to this recommendation, the UCR Program expanded its collection of data to include more details about the incidents in which law enforcement officers were killed or assaulted in the line of duty. Using this comprehensive set of data, the FBI began in 1972 to produce two reports annually, the *Law Enforcement Officers Killed Summary* and the *Analysis of Assaults on Federal Officers*. These two reports were combined in 1982 to create the annual publication, *Law Enforcement Officers Killed and Assaulted*.

The UCR Program's Hate Crime Statistics Program

Data provided

The hate crime data collected and published by the UCR Program comprise a subset of information that law enforcement agencies submit to the program—i.e., the information is separate from the routine Summary UCR submission. In addition, in hate crime reporting, there is no Hierarchy Rule. Offense data (not just arrest data) for intimidation and destruction/damage/vandalism of property should be reported. All reportable bias-motivated offenses should be reported regardless of whether arrests have taken place.

The types of hate crimes reported to the Hate Crime Statistics Program (i.e., the biases that motivated the crimes) are further broken down into more specific categories. As collected for each hate crime incident, the aggregate data in this report include the following: offense type, number of victims, location, bias motivation, victim type, number of victims, number of offenders, and the race of the offenders.

- Incidents and offenses—Crimes reported to the FBI involve those motivated by biases based on race, religion, sexual orientation, ethnicity/national origin, and disability.

- Victims—The victim of a hate crime may be an individual, a business, an institution, or society as a whole.

- Offenders—Law enforcement specifies the number of offenders and, when possible, the race of the offender or offenders as a group.

- Location type—Law enforcement may specify one of 25 location designations, e.g., residences or homes, schools or colleges, or parking lots or garages.

- Hate crime by jurisdiction—Includes data about hate crimes by state and agency.

Collection design

The designers of the Hate Crime Statistics Program sought to capture information about the types of bias that motivate crimes, the nature of the offenses, and some information about the victims and offenders. In creating the program, the designers recognized that hate crimes are not separate, distinct crimes; instead, they are traditional offenses motivated by the offender's bias (for example, an offender assaults a victim because of a bias against the victim's race). After much consideration, the developers agreed that hate crime data could be derived by capturing the additional element of bias in those offenses already being reported to the UCR Program. Attaching the collection of hate crime statistics to the established UCR data collection procedures, they concluded, would fulfill the directives of the Hate Crime Statistics Act without placing an undue additional reporting burden on law enforcement and, in time, would develop a substantial body of data about the nature and frequency of bias crimes occurring throughout the Nation.

Collection guidelines

More information about hate crime data submissions is provided in the UCR Program's *Hate Crime Data Collection Guidelines*. The program's Hate Crime Statistics Program also provides support and encourages agencies to call with any questions (888-827-6427).

More about the Hate Crime Statistics Program

On April 23, 1990, Congress passed the Hate Crime Statistics Act, which required the Attorney General to collect data "about crimes that manifest evidence of prejudice based on race, religion, sexual orientation, or ethnicity." The Attorney General delegated the responsibilities of developing the procedures for implementing, collecting, and managing hate crime data to the Director of the FBI, who in turn assigned the tasks to the UCR Program. Under the direction of the Attorney General and with the cooperation and assistance of many local and state law enforcement agencies, the UCR Program created the Hate Crime Statistics Program to comply with the congressional mandate.

Subsequent changes to the Hate Crime Statistics Program

- In September 1994, lawmakers amended the Hate Crime Statistics Act to include bias against persons with disabilities by passing the Violent Crime and Law Enforcement Act of 1994. The FBI started gathering data for the additional bias type on January 1, 1997.

- The Church Arson Prevention Act, which was signed into law in July 1996, removed the sunset clause from the original statute and mandated that the collection of hate crime data become a permanent part of the UCR Program. (See Hate Crime Statistics Act for referenced legislation, as amended.)

CLOSING CASES VS. CLEARING CASES

A pending case is one not yet finished. In law enforcement work, it means a case is being actively investigated with reports due at regular intervals.

Closing cases should not be confused with clearing cases. A case is closed when it is no longer investigated and is not assigned to an investigator. A closed case can be either solved or unsolved. Closing a case is merely an administrative procedure and not an investigative accomplishment.

All investigations should be closely supervised to determine if they are being properly conducted. When all facts of an investigation have been reported and no other action appears logical, the case may be closed.

A case is "cleared by arrest" when one or more persons are arrested, charged with the commission of the offense, and turned over to the court for prosecution (whether following arrest, court summons, or police notice). An offense should be considered "cleared by arrest" when one offender is apprehended and held for prosecution even though two or more individuals were jointly involved in the commission of the offense. The arrest of one person may clear several offenses; on the other hand, the arrest of several persons may clear but one offense.

Exceptional clearances

Cases may be cleared by exceptional means even if no arrest is made. In many instances, the law enforcement agency has exhausted all leads and has done everything possible to clear a case; however, identification of the offender is an essential factor in every "exceptional clearance."

For a case to be exceptionally cleared:

- The investigation must have clearly established the identity of the offender.
- Enough information must be present in order to obtain prosecution of the offender.
- The exact location of the offender must be known.
- Some reason outside law enforcement control must prevent the department from arresting, charging, and prosecuting the individual. Some examples of exceptional clearances are the following:
    - Suicide of the offender.
    - Double murder (two persons kill each other).
    - Deathbed confession.
    - Offender justifiably killed by police or citizen.
    - Confession by offender already in custody or serving sentence.
    - An offender prosecuted in another city for a different offense; or extradition is denied.

In all cases, if the offense is to be considered "exceptionally cleared," the perpetrator must be identified and an attempt at arrest made. In addition, the recovery of property alone does not "exceptionally clear" a case. Therefore, an "exceptionally cleared" case may be in either a closed or pending status.

Once the status of a case has been determined, it should be entered on the Incident/Offense Report by the Central Records supervisor.

CRIME STATISTICS FOR DECISIONMAKING

The law enforcement community has an ever-increasing need for timely and accurate data for a variety of purposes such as planning, budget formulation, resource allocation, assessment of police performance, and the evaluation of experimental programs. The information in this section focuses on the use, method of computation, and limitations of basic crime indicators employed by the Uniform Crime Reporting (UCR) Program. These indicators can aid law enforcement administrators in the performance of their duties and serve as forerunners for the implementation of more sophisticated analytical tools.

Volume, rate, and trend are basic crime indicators used in the UCR Program. Each statistic provides a different perspective of the crime experience known to law enforcement officials.

Volume

Crime volume is a basic indicator of the frequency of known criminal activity. In analyzing offense data, the user should be aware that a UCR volume indicator does not represent the actual number of crimes committed; rather, it represents the number of reported offenses. With respect to murder and nonnegligent manslaughter, forcible rape, and aggravated assault, it represents the number of known victims. For robbery, burglary, larceny-theft, motor vehicle theft, and arson, it represents the number of known incidents. The crimes are divided into two components: violent and property crimes. The violent crime total includes murder and nonnegligent manslaughter, forcible rape, robbery, and aggravated assault, while the property crime total encompasses burglary, larceny-theft, motor vehicle theft, and arson.

Offense and arrest rates

Crime rates are indicators of reported crime activity standardized by population. They are more refined indicators for comparative purposes than are volume figures. The UCR Program provides three types of crime rates: offense rates, arrest rates, and clearance rates.

An offense rate, or crime rate, defined as the number of offenses per 100,000 population, is derived by first dividing a jurisdiction's population by 100,000 and then dividing the number of offenses by the resulting figure.

Example:
a. Population for jurisdiction, 75,000
b. Number of known burglaries for jurisdiction for a year, 215

Divide 75,000 by 100,000 = .75
Divide 215 by .75 = 286.7
The burglary rate is 286.7 per 100,000 inhabitants.

The number .75 can now be divided into the totals of any offense category to produce a crime rate for that offense. The same procedure may be used to obtain arrest rates per 100,000 inhabitants.

Clearance rates

A clearance rate differs conceptually from a crime or arrest rate in that both the numerator and denominator constitute the same unit of count (i.e., crimes). Unlike a crime or arrest rate, a clearance rate represents percentage data. A clearance rate is, therefore, equivalent to the percentage of crime cleared.

The percentage of crimes cleared by arrest and exceptional means (i.e., clearance rate) is obtained first by dividing the number of offenses cleared by the number of offenses known and then multiplying the resulting figure by 100.

Example:
a. Number of clearances in robbery, 38
b. Number of total robberies, 72

Divide 38 by 72 = .528
Multiply .528 x 100 = 52.8 percent
The clearance rate for robbery is 52.8 percent.

Crime trends

Crime trend data from one period to the next are presented in the UCR Program's annual report *Crime in the United States* and other UCR publications. A crime trend represents the percentage change in crime based on data reported in a prior equivalent period. These statistics play a prominent role for both offense and arrest analyses. Trends can be computed for any time frame, such as months, quarters, or years. The UCR Program employs two types of trend statistics: volume trends and rate trends. Local agencies can compute trends for a given offense for any period of time.

Trend computation requires two numbers representing the two comparable time frames. In the example below, (earlier) represents the crime volume or rate for the first period or earlier period of comparison, and (later) represents the corresponding crime volume or rate for the second period or later period of comparison. The trend is computed by first subtracting (earlier) from the (later), then dividing the difference by (earlier), and finally by multiplying the quotient by 100.

Example:
a. Murders in the jurisdiction for January through June, last year, 21
b. Murders in the jurisdiction for January through June, this year, 29

Subtract:

$$\begin{array}{r} 29 \\ \underline{-21} \\ 8 \end{array}$$

Notice that "8" is an increase over the past year.

Divide 8 by 21 = .381
Always divide the difference by the total in the earlier time period.

Multiply .381 by 100 = 38.1 percent.

The volume trend in murder is an increase of 38.1 percent for the first 6 months of this year as compared to the first 6 months of the prior year. Note that there can never be a decline of more than 100 percent. Also, if the figure for a prior period is zero, a trend computation cannot be made.

This same computation will yield rate trends if rate figures are substituted for volume figures in the above formula.

Law enforcement employee rates

Law enforcement employee rates are expressed as the number of employees per 1,000 inhabitants. To compute such a rate, divide the jurisdiction's population by 1,000 and divide the number of employees in the law enforcement agency by this number.

Example:
a. The jurisdiction's population, 75,000
b. The agency's number of employees, 102

Divide 75,000 by 1,000 = 75
Divide 102 by 75 = 1.36
The employee rate is 1.36 employees per 1,000 inhabitants.

Other indicators

Another commonly computed crime indicator is a population-at-risk rate. In essence, a population-at-risk rate is a refined crime rate measured in units that are most inclined to be victimized. The burglary rate based on the gross number of inhabitants may not be as accurate as a population-at-risk rate based on the number of units subject to be burglarized (residences and/or commercial establishments). Below are some of the common indicators of population-at-risk rates for different offenses:

a. Female Rape—The number of females 12 and older

$$\text{Rate} = \frac{\text{number of rapes}}{\text{number of females 12 and older}} \text{ x } 100{,}000$$

b. Commercial burglary—the number of commercial establishments

$$\text{Rate} = \frac{\text{number of commercial burglaries}}{\text{number of commercial establishments}} \text{ x } 100{,}000$$

c. Residential burglary—the number of residences

$$\text{Rate} = \frac{\text{number of residential burglaries}}{\text{number of residences}} \times 100{,}000$$

d. Motor vehicle theft—the number of motor vehicle thefts per 100,000 registered vehicles

$$\text{Rate} = \frac{\text{number of motor vehicle thefts}}{\text{number of registered vehicles}} \times 100{,}000$$

Data limitations

When analyzing UCR statistics, direct agency-to-agency comparisons should be guarded against. Such comparisons could be misleading unless demographic differences between jurisdictions are taken into account. Every community has a unique social, ethnic, and economic configuration that may affect its crime statistics. These dissimilarities may bias the results of any comparative analysis between agencies. A jurisdiction's crime situation is complex and cannot always be treated superficially as it might be in direct agency-to-agency comparisons.

In general, the decision to use any indicator for analysis purposes must be made with care. The UCR indicators discussed previously have utility for law enforcement administrators; however, they must be used with caution. No single indicator is a panacea for crime analysis. Instead, decisions that law enforcement administrators are called upon to make require a multifaceted analytical approach.

GLOSSARY OF COMMONLY USED ACRONYMS

APB	Advisory Policy Board
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
CHRI	Criminal History Record Information
CJIS	Criminal Justice Information Services
CSA	CJIS Systems Agency
CSO	CJIS Systems Officer
FBI	Federal Bureau of Investigation
FFL	Federal Firearms Licensee
IACP	International Association of Chiefs of Police
IAFIS	Integrated Automated Fingerprint Identification System
III	Interstate Identification Index
LEOKA	Law Enforcement Officers Killed and Assaulted
NCIC	National Crime Information Center
N-DEx	The Law Enforcement National Data Exchange
NFF	National Fingerprint File
NGI	Next Generation Identification
NIBRS	National Incident-Based Reporting System
NICS	National Instant Criminal Background Check System
NTN	NICS Transaction Number
POC	Point of Contact
RMS	Records Management System
UCR	Uniform Crime Reporting or Uniform Crime Reports