It's been called the lifeline of law enforcement—an electronic clearinghouse of crime data that can be tapped into by virtually every criminal justice agency nationwide, 24 hours a day, 365 days a year.

The **National Crime Information Center**, or NCIC, was launched on January 27, 1967 with five files and 356,784 records. By the end of Fiscal Year (FY) 2011, NCIC contained 11.7 million active records in 19 files. During FY 2011, NCIC averaged 7.9 million transactions per day.

NCIC helps criminal justice professionals apprehend fugitives, locate missing persons, recover stolen property, and identify terrorists. It also assists law enforcement officers in performing their official duties more safely and provides them with information necessary to aid in protecting the general public.

About the records: The NCIC database currently consists of 21 files. There are seven property files containing records of stolen articles, boats, guns, license plates, parts, securities, and vehicles. There are 14 persons files, including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; U.S. Secret Service Protective; Gang; Known or Appropriately Suspected Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction. The system also contains images that can be associated with NCIC records to help agencies identify people and property items. The Interstate Identification Index, which contains automated criminal history record information, is accessible through the same network as NCIC. See details on the files.

How NCIC is used: Criminal justice agencies enter records into NCIC that are accessible to law enforcement agencies nationwide. For example, a law enforcement officer can search NCIC during a traffic stop to determine if the vehicle in question is stolen or if the driver is a wanted by law enforcement. The system responds instantly. However, a positive response from NCIC is not probable cause for an officer to take action. NCIC policy requires the inquiring agency to make contact with the entering agency to verify the information is accurate and up-to-date. Once the record is confirmed, the inquiring agency may take action to arrest a fugitive, return a missing person, charge a subject with violation of a protection order, or recover stolen property.

Cooperation is key: NCIC has operated under a shared management concept between the FBI and federal, state, local, and tribal criminal justice users since its inception. There are two facets to the shared management concept—policy and functional.

The policy facet provides a means for user input on NCIC policy through the Criminal Justice Information Services (CJIS) Advisory Policy Board. The board enables NCIC users to make

recommendations to the FBI Director for policy and operational enhancements to the system. The CJIS Division actively promotes the use of the system and its benefits through daily interaction with users—whether by phone, video teleconference, or e-mail; attendance at meetings and seminars; and via the advisory process.

The functional facet provides a means for agencies to access NCIC. The FBI provides a host computer and telecommunication lines to a single point of contact 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. Those jurisdictions, in turn, operate their own computer systems, providing access to nearly all local criminal justice agencies and authorized non-criminal justice agencies nationwide. The entry, modification, and removal of records are the responsibility of the agency that entered them. The CJIS Division serves as the custodian of NCIC records.

Security and quality controls: The head of the CJIS Systems Agency—the criminal justice agency that has overall responsibility for the administration and usage of NCIC within a district, state, territory, or federal agency—appoints a CJIS systems officer (CSO) from its agency. The CSO is responsible for monitoring system use, enforcing system discipline and security, and assuring that all users follow operating procedures. NCIC policy establishes a number of security measures to ensure the privacy and integrity of the data. The information passing through the network is encrypted to prevent unauthorized access. Each user of the system is authenticated to ensure proper levels of access for every transaction. To further ascertain and verify the accuracy and integrity of the data, each agency must periodically validate its records. Agencies also must undergo periodic audits to ensure data quality and adherence to all security provisions.

For Law Enforcement: Additional information and documentation on NCIC can be found on the FBI's Law Enforcement Online (LEO) website.