

NATIONAL CRIME INFORMATION CENTER (NCIC)

AN OVERVIEW



July 2022

What is the NCIC?

The National Crime Information Center (NCIC) is a system of documented criminal justice information available to law enforcement and criminal justice agencies nationwide, 24 hours a day, 365 days a year. The goal of the NCIC System is to assist law enforcement in apprehending fugitives, locating missing persons and identifying stolen property. This goal includes investigative intelligence pertaining to gangs, domestic and foreign terrorist, and individuals who pose a physical threat to law enforcement and criminal justice personnel.

Files

The NCIC database consists of 22 files. The seven property files are the Article, Boat, Gun, License Plate, Securities, Vehicle, and Vehicle and Boat Part Files. The 15 person files are the Extreme Risk Protection Order, Foreign Fugitive, Gang, Identity Theft, Immigration Violator, Missing Person, National Instant Criminal Background Check System Denied Transaction, the National Sex Offender Registry, Protection Order, Protective Interest, Supervised Release, Threat Screening Center, Unidentified Person, Violent Person, and Wanted Person Files. In addition, the database contains images that can be associated with NCIC records to assist agencies in identifying people and property items. The Interstate Identification Index, which contains automated criminal history record information, is also accessible through the same network as the NCIC.

Management

Since its inception, the NCIC has operated under a shared management concept between the Federal Bureau of Investigation (FBI) and state and federal criminal justice agencies. The general policy concerning the philosophy, concept, and operational principles of the System is based upon the recommendations of the CJIS Advisory Policy Board to the Director of the FBI. Top administrators from local, state, territory, tribal, and federal criminal justice agencies throughout the United States make up this advisory process.

The FBI maintains the host computer and provides a telecommunication network to the CJIS Systems 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. A CSA is a criminal justice agency that has overall responsibility for the administration and usage of the NCIC within a district, state, territory, or federal agency. Those 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 data or search millions of records for persons and property.

How the NCIC is used

Criminal justice agencies enter records into the NCIC, which, in turn, are accessible to law enforcement agencies nationwide. For example, a law enforcement officer can conduct an inquiry of NCIC during a traffic stop to determine if the vehicle in question is stolen or if the driver is a wanted person, and the NCIC System responds instantly. However, a positive response from the 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, recover stolen property, or deny the purchase of a firearm or access to explosives.

System Security and Quality Controls

The head of the CSA 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, which are 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.