Technical Bulletin

featuring emerging technologies in criminal justice information management

1998 Issue Number 2

From the Inkpad to the Mousepad: IAFIS and Fingerprint Technology at the Dawn of the 21st Century

By Eric C. Johnson
SEARCH

The use of fingerprints for identification purposes began at the end of the 19th century and revolutionized crime fighting. As the 20th century comes to a close, ongoing developments in fingerprint technology promise to revolutionize law enforcement just as the inkpad did nearly 100 years ago.

In July 1999, law enforcement agencies throughout the country will begin to have access to the Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System (IAFIS), a national on-line fingerprint and criminal history database with identification and response capabilities considered unattainable less than a decade ago.

Justice agencies that now wait several weeks for the FBI to respond to identification requests will have the same information in their hands in just 2 hours when requests are submitted to IAFIS electronically. Agencies that submit identification requests for noncriminal justice use such as pre-employment background checks and licensing purposes will have the information returned to them in only 24 hours when submitted electronically.

IAFIS will allow the FBI to process 62,000 10-print searches per day, more than enough capability to respond to the 51,000 fingerprint cards that are currently submitted to the Bureau daily. In addition, IAFIS will be able to search latent prints obtained at crime scenes against its master database of known criminal suspects. When completed, IAFIS will have cost $640 million, the U.S. Justice Department's most expensive project ever, according to the FBI's Douglas J. Domin, Deputy Assistant Director of Operations, who is responsible for the transfer of the Bureau's fingerprint services to IAFIS.

Three Segments of IAFIS

IAFIS consists of three basic integrated segments: the Automated Fingerprint

Bureau of Justice Assistance, SEARCH Explore New Technologies

The SEARCH *Technical Bulletin* is a publication designed to examine emerging technologies in criminal justice information management. Research and publication of the *Bulletin* is funded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

The *Bulletins* identify, describe and assess new and emerging technologies that have existing or potential application in criminal justice information management. They alert practitioners to the existence of technologies which can benefit their management of information.

To submit an article for publication in the *Technical Bulletin*, please contact SEARCH, The National Consortium for Justice Information and Statistics, at (916) 392-2550.

Publication Funded by
BJA Bureau of Justice Assistance

Identification System (AFIS), the Interstate Identification Index (III) and Identification Tasking and Networking (ITN). Here is how IAFIS will work when operational:

An individual taken into custody at the local level is fingerprinted on a live-scan fingerprinting terminal. Using store-and-forward technology[1], copies of the digitized prints, along with the suspect's personal information — such as name, address, birth date, social security number and type of offense — are transmitted through the state's law enforcement network to the state fingerprint repository. There, the prints are electronically checked for matches and are stored. Copies of the prints are also transmitted along with the personal information through the FBI's Criminal Justice Information Services (CJIS) Division's Wide-Area Network (WAN) to the FBI's fingerprint repository, maintained by CJIS in Clarksburg, West Virginia. The CJIS WAN, operational since 1997, is comprised of high-end communications equipment, encryption components and firewalls installed in all 50 states. It was designed with enough communications bandwidth to support a daily traffic load of more than 74,000 fingerprint package transmissions and hundreds of thousands of other transactions.[2]

This is where IAFIS begins its work. The state submission arrives in the form of an email carrying attachments with compressed fingerprint and mugshot images and a text file with the suspect's personal information. IAFIS' ITN component — the network's "traffic cop," according to Mr. Domin — opens the email transmission and conducts a quality check to make sure it is formatted for the correct transaction type and to determine whether the required number of records are present. A technician then conducts a second quality control examination before initiating the search process.

Using the suspect's personal information, ITN conducts a III subject search. III, created for the National Crime Information Center (NCIC) before being incorporated into the Identification Division Automated System (IDAS) when it was implemented in 1989, contains the criminal histories or "rap sheets" of around 30 million offenders.

"The III search uses a sophisticated matching algorithm that looks for a name, birth date, social security number and other information," said Mr. Thomas J. Roberts, IAFIS Assistant Program Manager. "When determining the likelihood of identification, it can recognize birth dates or social security numbers that almost match except for two numbers being transposed, for example."

If a matching file is found, its fingerprint images are transmitted to a technician, who will compare side-by-side the database prints to those submitted by the law enforcement agency to verify the suspect's identity. The III file also will be automatically updated with the new criminal history information.

If no match results from the subject search, ITN will utilize the FBI's AFIS to search the Bureau's 40 million 10-print digitized files. The system can examine 3 million fingerprints per second, according to Mr. Domin. AFIS may return one candidate or a list of possible matches. A technician reviews the prints to make the final identification determination. "The technician then simply clicks on a button indicating whether or not the subject has been identified, and the system generates a return message automatically," said CJIS Computer Specialist Lawrence Jolma.

Once an identification is achieved, the III database is queried to establish whether the suspect has an existing

The *Technical Bulletin* is published by SEARCH, The National Consortium for Justice Information and Statistics, with funding from the Bureau of Justice Assistance, U.S. Department of Justice.

This document was prepared under grant number 97-DD-BX-0077, provided by the Bureau of Justice Assistance, U.S. Department of Justice. The points of view or opinions stated in the document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

SEARCH is located at 7311 Greenhaven Drive, Suite 145, Sacramento, California 95831, (916) 392-2550.

criminal history or outstanding warrants. If no match is found from either the subject search or the fingerprint search, the suspect's name, criminal history and fingerprints are added to the respective databases, an FBI identification number is assigned to the suspect, and the agency which requested the identification is notified of the search results and the new number. Mr. Roberts said that based on recidivism patterns, seven out of every 10 individuals searched for in the FBI's files will most likely be found. Mr. Domin estimated that IAFIS will prevent the release of the 10,000 to 30,000 fugitives freed each year because of extended delays in establishing their true identities and warrant status.

If the submitted prints are of higher quality than those on file, the FBI's AFIS will automatically replace the encoded minutiae on file with minutiae extracted from submitted images. IAFIS technicians also can examine 10-print sets and replace one or more of the images in the set if the submitted prints are of better visual quality than the fingerprints on file.

For urgent information requests, the entire IAFIS process is expected to take 2 hours from the time prints generated on live-scan devices reach the FBI until a return message is generated and transmitted to the submitting agency, and 24 hours for non-urgent end-to-end live-scan transmissions. The implementation of IAFIS culminates a decades-long effort to merge the power of technology with the certainty of fingerprint identification to create a system that can effectively respond to the growing needs of state- and local-level law enforcement agencies.

IAFIS Origins

The FBI, founded in 1908, has maintained the nation's fingerprint repository since 1924, when it assumed control of more than 800,000 print files consolidated from the National Bureau of Criminal Identification and from Leavenworth Penitentiary.[3]

For almost 50 years, the FBI relied almost exclusively on a fingerprint classification system devised at the end of the 19th century by Sir Edward Henry, Assistant Commissioner of the Criminal Investigation Department at Scotland Yard, to categorize and match its prints. The Henry Fingerprint Classification System classifies fingerprints by ridge formations and other unique identifying factors.[4] The Bureau experimented with and implemented early versions of automated fingerprint systems in the early- and mid-1970s for internal file keeping, but all prints transmitted to the FBI by state repositories and other law enforcement agencies were sent by mail. FBI technicians also used the Henry classification system and visual examinations to make identification determinations.

Fingerprint technology evolved to such a degree that by the mid-1980s, it became feasible for fingerprint repositories in states and large cities to automate portions of their fingerprint services. A handful of manufacturers had developed and enhanced automated fingerprint identification systems using technology developed with the support of the FBI and Japan's national police.

Virtually all agencies that contributed fingerprints to the state repositories obtained them manually using ink. The inked 10-print cards were mailed to the repositories and then were digitized by a card reader that extracted the fingerprint's minutiae or identifying factors so an electronic search for matches could be conducted. The system produced a list of candidates, and a technician would make the final match determination. Results were returned by mail to the contributing agencies.

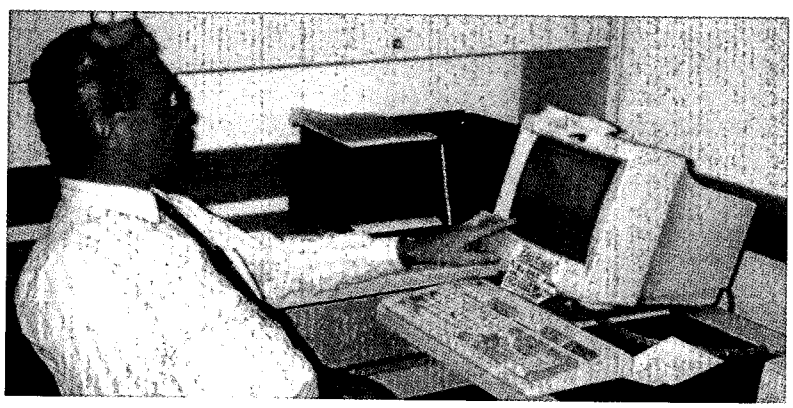
Automated services were generally limited to systems maintained by state repositories and by large police agencies. A few intrastate and regional networks developed that allowed the exchange of fingerprint data, such as the Western Identification Network (WIN), which connected nine western states.[5] Because WIN participants used equipment manufactured by the same vendor (NEC Technologies), participating repositories could exchange information electronically. Larger-scale or nationwide networks were virtually impossible to establish because of the incompatibility of different vendors' systems that had been installed in repositories around the county, making it impossible for one state's fingerprint repository to electronically utilize data stored in another state's system that operated a

different vendor's AFIS. Arizona, for example, could no longer participate in WIN because it purchased an AFIS manufactured by Sagem Morpho Inc., which could not electronically interact with WIN's NEC systems.

The number of states utilizing AFIS technology continued to grow in the latter half of the 1980s. The FBI's NCIC Advisory Policy Board (APB) — which consisted of representatives of federal, state and local criminal justice agencies — reported to then-Director William Sessions that improvements were necessary to keep pace with automation efforts at the state level. In 1989, Director Sessions asked the APB to expand its advisory role to include fingerprint identification services and to provide the FBI with advice on necessary identification services upgrades, according to Mr. Joseph Bonino, commanding officer of the Los Angeles Police Department's Jail Division and an APB member since 1988. (The NCIC APB was reorganized as the Criminal Justice Information Services APB in 1994. Mr. Bonino has served as Chair of the CJIS APB since then.)

The APB formed a subcommittee (called the Identification Services Task Group) to examine the operations of the FBI's Identification Division and to recommend improvements. The task group's 27 recommendations comprised the "Identification Division Revitalization" report submitted to the director in February 1990 that became the foundation for the development of IAFIS, Mr. Bonino said.

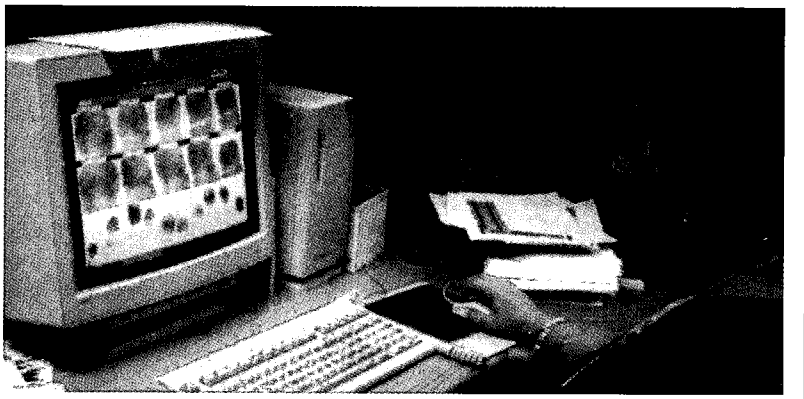
Live-Scan Field Representative Lewis R. Hayden of the Bureau of Criminal Identification and Information, Office of the Attorney General in California, demonstrates how fingerprints are taken on a live-scan device, an Identix TouchPrint located at the county jail in San Joaquin County.



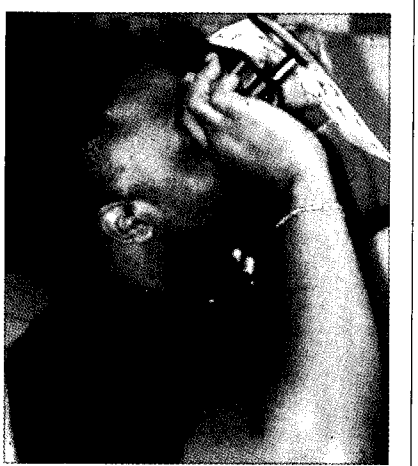
Lt. Thomas H. Davis of the San Joaquin County, California, Sheriff's Department, examines a computerized list of fingerprint images and related data that were electronically transmitted from the San Joaquin County Jail to California's fingerprint repository in Sacramento.

One of the major recommendations in the APB task group's report proposed that the FBI take the lead in developing a standard for electronic fingerprint image communications. The task group believed a common national standard for the capture and transmission of fingerprint images and associated identification data would help alleviate the problem of incompatible, proprietary AFIS systems, which could not exchange and share information. Working with the National Institute for Standards and Technology and federal, state and local criminal justice representatives, the FBI held a series of workshops from 1990 to 1992 to discuss and agree upon the required standard. The standard, officially designated the *Data Format for the Exchange of Fingerprint Informa-*

pictured here, uses state-of-the-art technology



Criminal Identification Specialist Mary Faraj of the Bureau of Criminal Identification and Information, Office of the Attorney General in California, conducts a quality control examination of computerized fingerprint images that were electronically transmitted to the state repository in Sacramento.



A criminal identification specialist at the Bureau of Criminal Identification and Information, Office of the Attorney General in California, uses a magnifying device to examine a printed fingerprint image. The manual examination of fingerprint images demonstrated here is becoming less common as more law enforcement agencies turn to computer-based fingerprint services.

tion, was approved by the American National Standards Institute and published in November 1993.[6] Most AFIS and live-scan equipment vendors now support this standard, making it easy for federal, state and local criminal justice agencies to procure IAFIS-compatible systems.

Based on the recommendations contained in the task group's report, the FBI prepared and issued procurement documents seeking contractors to build the ITN portion of IAFIS and to update III's hardware and software platforms. III also needed more functionality so it could store digital mugshot images. The Bureau selected Litton/PRC Inc. of McLean, Virginia, to develop the ITN, IAFIS' work-flow manager. Science Applications International Corp. (SAIC), also of McLean, Virginia, was selected to upgrade III.

The AFIS portion of IAFIS was a different matter. It was unclear whether the technology available in the early 1990s could manage a fingerprint database as large as the one maintained by the FBI. The world's largest at the time — maintained by the California Department of Justice — held just over 5 million 10-print cards. The FBI's fingerprint database was almost seven times as large.

The FBI decided to follow the U.S. Defense Department's practice and conduct its own version of a "fly-off," a process during which grants are given to aircraft manufacturers to assemble airplane prototypes which then compete against each other in design competitions.

For the AFIS segment of IAFIS, three contractors — Lockheed Martin Corp., TRW Inc. and Unisys Corp. — were each given grants of approximately $10 million from the FBI in May 1994 to develop Basic Demonstration Models (BDMs), which were scaled-down versions of their proposed systems. When the BDMs were ready for competition, the FBI provided 500,000 10-print cards and latent prints for a blind-test design competition between the contractors. The Bureau was seeking a system that could complete a search of its 10-print fingerprint database in 15 minutes or less, and one that could respond in 2 hours or less to electronically submitted information requests while also handling latent print services. In January 1996, Lockheed Martin Information Systems of Orlando, Florida, was awarded a 6-year, $109 million contract to develop the AFIS portion of IAFIS.

The first IAFIS software to be completed and placed into operation was the Stand-Alone Image Storage and Retrieval System (ISR-SA), developed by PRC Inc., which became operational on October 6, 1997. ISR-SA allowed the FBI to access its Fingerprint Image Master File

and to retrieve sets of images for on-screen comparison.

The FBI originally planned a single-step IAFIS assembly that would provide initial operational capability in 1998 and full operational capability beginning in mid-1999. However, to reduce overall development risk, and to allow users to enjoy partial benefits and incremental functionality from the system while awaiting its completion, the FBI decided instead to assemble the system in six steps or "builds" designated as A through F. Users could become familiar with portions of the system as it grew rather than having to learn how to use the entire system at one time. IAFIS will become fully operational as a system at the completion of Build F.

Pilot Program

During Build A, a pilot program was established that allowed the first electronic transmission of fingerprints to the FBI. The contributing agency was the Boston, Massachusetts, Police Department, which implemented an integrated electronic imaging identification system after an analysis of operations found that officers were wasting 40,000 hours per year transporting prisoners from the city's 11 police districts to a central booking facility.

Comnetix Computer Systems, a Canadian firm, won a $2.5 million contract to install live-scan fingerprint and mugshot booking workstations at the 11 district police stations and a central server at police headquarters. Since its implementation in October 1994, the system has reportedly saved Boston more than $1 million in labor and transportation costs, and the equivalent of two officers per shift — freed from transporting prisoners to central booking at police headquarters — are back on the streets.[7] It was up and running when the FBI came looking for an agency to participate in its IAFIS pilot program. "We were in the position to electronically transmit fingerprints and the FBI needed an agency to participate in the pilot program, so we did," said Deputy Superintendent Bill Casey.

The first prints, those of an armed robbery suspect, were transmitted August 23, 1995. The FBI received the images within 2 minutes and contacted Boston police 2 hours later to report that it had identified the prints, matched them to the suspect, and found that he was a fugitive following a previous arrest in North Carolina.[8] Boston has moved beyond the pilot program and was sending an average of about 35 live-arrest print files a day to the FBI in October 1998, according to Bureau statistics.

Until IAFIS goes online, the prints and accompanying criminal histories are transmitted through the CJIS WAN to a device called the Electronic Fingerprint Image Printer Server (EFIPS), which reproduces them on 10-print paper cards for processing by the FBI's IDAS semi-automated system. FBI personnel conduct quality-control inspections on the prints, which are then classified and submitted to IDAS, which produces a list of likely candidates for verification. A service provider compares the submitted prints with those on file for final determination and results are returned electronically to the submitting agency. The process averages about 8 days, according to Mr. Jolma.

Current State Transmissions

The FBI uses the same process to respond to the needs of states that were ready to transmit prints electronically to the Bureau following their own internal efforts to automate and integrate fingerprint and criminal history data and services. At this writing, California, Georgia and Florida are most active among the states in transmitting fingerprint files electronically to the FBI.

— California

California, which has had an operational AFIS since its Digital Image Retrieval System (developed by NEC Technologies) was implemented in 1985, electronically submitted an average of about 815 live-arrest fingerprint files a day to the FBI in October 1998. In 1997, California's AFIS underwent a $35 million upgrade that transitioned the system from optical to Redundant Array of Independent Disks (RAID) storage technology, which protects against full-scale system failure by maintaining data on multiple hard drives rather than on a single large disk.

California's CAL-ID program seeks to install a live-scan fingerprint device in all 58 counties in the state and perhaps in other facilities such

as those that deal with juvenile justice and corrections. Agencies electronically forward fingerprint files to the state's fingerprint repository in Sacramento, which transmits the files through the CJIS WAN to the FBI. California maintains fingerprint files on almost 9 million individuals.

— *Georgia*

Georgia, which purchased its first AFIS from NEC Technologies in 1987, transmitted approximately 350 prints per day to the FBI in October 1998. Georgia's AFIS, the first in the world to integrate fingerprint identification and criminal history updates, is managed by the Georgia Bureau of Investigation. It includes five subsystems:

- The Input Subsystem, which consists of two NEC fingerprint readers that scan print images and that perform minutiae detection;
- the Matching Subsystem, which takes minutiae points from submitted prints and looks for matches with database prints;
- the Digital Subsystem, which holds the fingerprint images after potential match candidates are located;
- the Transaction Network, a local area network (LAN) for data entry, transaction management and communications; and
- the Networked AFIS Transaction Management System, which supports fingerprint transmissions from local agencies to the FBI.

Georgia's initial AFIS cost $6.1 million. Two subsequent upgrades cost $5.2 million. The AFIS holds approximately 3.75 million fingerprints. It retains all 10 fingerprints for individuals who commit serious offenses, such as burglary. For less serious crimes, such as driving under the influence, only thumbprints are retained. Approximately 30 percent of the fingerprints supplied to the state AFIS from local agencies are submitted electronically. Almost two-thirds will be transmitted electronically by mid-1999.

— *Florida*

Florida has used Printrak equipment since it implemented its first AFIS in 1988. The AFIS is maintained as part of the state's Integrated Criminal History Network, which is directed by the Florida Department of Law Enforcement. Florida currently maintains live-scan devices in 29 counties or municipalities. Funding has been appropriated to purchase the devices for a total of 40 of Florida's 67 counties. Three other counties purchased their own live-scans.

During the booking process, a suspect's fingerprints are electronically transmitted to the state fingerprint repository in Tallahassee for identification verification. A response is returned to the submitting agency in approximately 15 minutes and the booking process proceeds. Once it is concluded, the suspect's complete arrest and fingerprint record is returned to the repository in Tallahassee, which forwards a copy to the FBI. Florida transmitted an average of about 460 fingerprint files to the FBI each day in October 1998. Florida's fingerprint repository holds the fingerprint records of approximately 1.5 million individuals. Its AFIS has the capacity to store 2.5 million 10-print records and 100,000 latent fingerprints.

The FDLE also maintains live-scan devices in the state's 20 juvenile assessment centers and in its five Department of Corrections' centers. Florida's current AFIS was implemented in October 1997 and cost the state $6.3 million.

Massive Transition Project

The transition of the world's largest fingerprint and criminal history databases to IAFIS is a massive undertaking that moves forward even as more than 50,000 print cards pour into the FBI for processing each day. "We can't let current activities slack just because we're in transition," said Mr. Jolma. A transition task force meets each morning to iron out not only hardware and software issues associated with the intricate IAFIS system, but also personnel matters such as training, work schedules and office assignments, he said. During the transition, FBI personnel attacked and eliminated a backlog of more than one million fingerprint cards that had been submitted for processing, according to Mr. Jolma.

In accordance with the FBI's preparation timeline, IAFIS will assume some operational capacity beginning in July 1999. When IAFIS becomes fully operational, the federal government will have completed its obligation under the

original IAFIS plan. However, for IAFIS to be completed as a national system (as opposed to a federal system) it is imperative for states, as IAFIS partners, to upgrade their internal fingerprint services so they can contribute and receive images and data in a timely fashion for the benefit of criminal justice and noncriminal justice information users nationwide, according to Mr. Gary R. Cooper, Executive Director of SEARCH, The National Consortium for Justice Information and Statistics.

Forty-nine states had automated fingerprint identification systems as of March 1998, according to the FBI.[9] "Some states are already sending us data, and other states are close to sending," said Mr. Jolma.

Those that do take advantage of IAFIS will have access to one of the most effective law enforcement tools ever created, one that would amaze not only those who first noticed the unique characteristics of fingerprints more than a century ago but also those who first considered the modernization of fingerprint services just a decade ago.

Endnotes

[1] The store-and-forward switching process allows the storage of a complete incoming data packet before it is sent out. The process is used when incoming and outgoing speeds differ.

[2] FBI Press Release.

[3] "The FBI's Approach to Automatic Fingerprint Identification," by Conrad S. Banner and Robert M. Stock, *FBI Law Enforcement Bulletin*, January-February 1975.

[4] The Henry system relies on eight basic fingerprint ridge formations, termed "minutiae" — dots, ending ridges, bifurcations or forks, enclosures, bridges, recurves, spurs and meeting ridges. Also utilized are the fingerprint's core or center point, and axis or general pattern direction.

[5] When established in 1989, the Western Identification Network (WIN) consisted of 9 associate or general member states. Associate members Alaska, Arizona, California and Washington maintained their own fingerprint databases and networked with other WIN participants. General members Idaho, Nevada, Oregon, Utah and Wyoming shared a database and search services provided by NEC Technologies (Source: "California Identification (CAL-ID) System and Remove Access Network (RAN) Status Report: 1989-1990," published by the California Department of Justice). In November 1998, WIN consisted of 7 "central-site" members (Alaska, Idaho, Montana, Nevada, Oregon, Utah, Wyoming) that share a database, and 2 "interface" members (California and Washington) that maintain their own databases but that provide WIN connectivity (Source: Gary Goad, WIN).

[6] ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information, sponsored by National Institute of Standards and Technology, published by American National Standards Institute, November 22, 1993.

[7] "Imaging: Prints Go Online, Cops Return to Streets," by Tod Newcombe, Features Editor, *Government Technology*, April 1996.

[8] Ibid.

[9] Integrated Automated Fingerprint Identification System (IAFIS) Program Overview, FBI, March 24, 1998.

Technical Bulletin
featuring emerging technologies in criminal justice information management

NONPROFIT ORG.
U.S. POSTAGE
PAID
Permit No. 1632
Sacramento, CA

SEARCH
The National Consortium for Justice Information and Statistics
7311 Greenhaven Drive, Suite 145 • Sacramento, California 95831
Telephone (916) 392-2550 • www.search.org