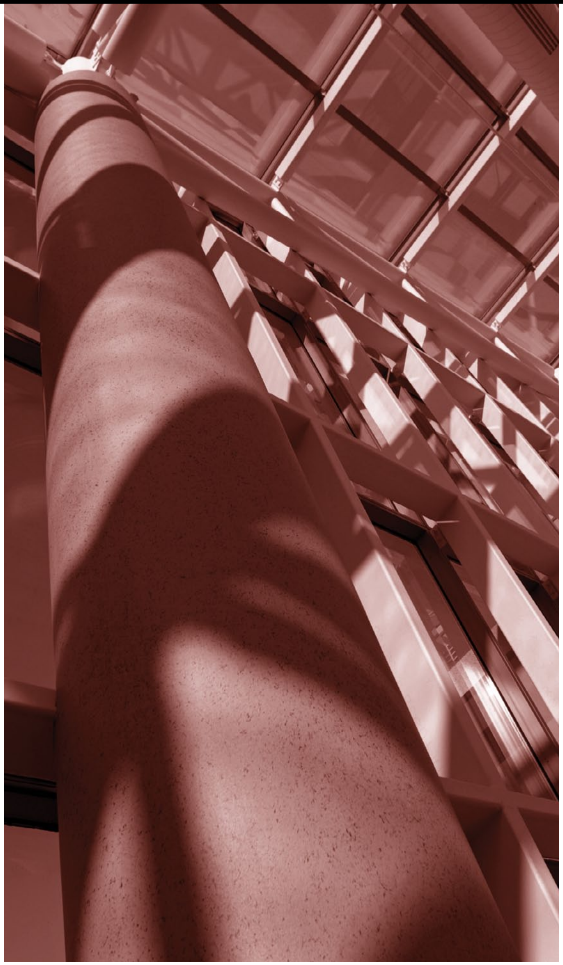
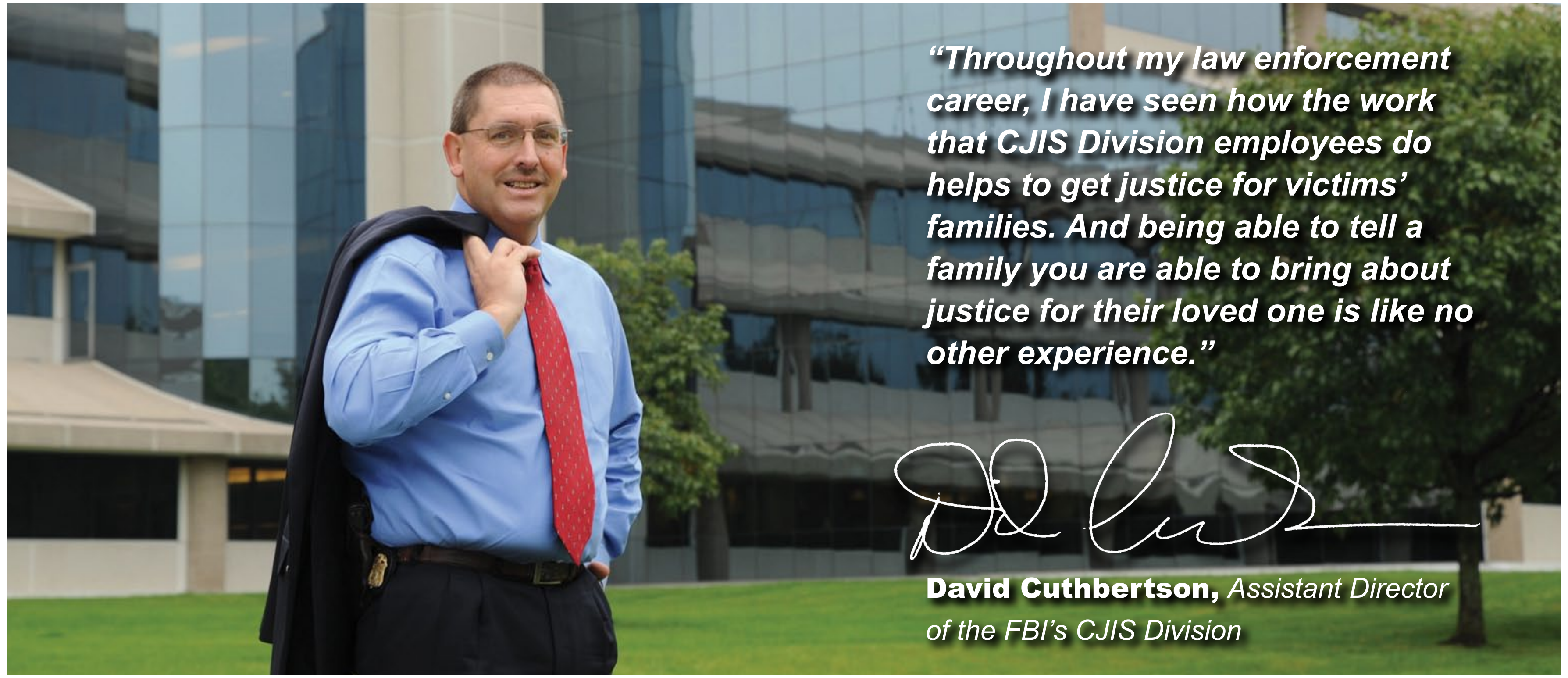
U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

THE POWER TO CONNECT • THE POWER TO IDENTIFY • THE POWER TO KNOW



CJIS

ANNUAL REPORT 2011



> *"Throughout my law enforcement career, I have seen how the work that CJIS Division employees do helps to get justice for victims' families. And being able to tell a family you are able to bring about justice for their loved one is like no other experience."*

David Cuthbertson, *Assistant Director of the FBI's CJIS Division*

As the newly appointed Assistant Director of the CJIS Division, I have the honor of presenting the 2011 edition of the *CJIS Annual Report*. This publication showcases the work of the Division's more than 2,500 employees as they provide vital criminal information services to our partners in the law enforcement, national security, and intelligence communities we serve. Highlights from Fiscal Year (FY) 2011 include the following accomplishments. The CJIS Division:

- Accommodated a continued rise in average daily fingerprint submissions, up from 42,203 in FY 1999 to nearly 140,000 in FY 2011.
- Processed an average of 7.9 million National Crime Information Center (NCIC) transactions per day with a new single-day record set on July 29 when the NCIC processed nearly 9.8 million transactions.
- Conducted more than 14 million background checks via the National Instant Criminal Background Check System (NICS).
- Accomplished 49 Foreign Biometric Exchange missions partnering with other countries to obtain biometric records and related information for analysis and comparison within the Integrated Automated Fingerprint Identification System (IAFIS).
- Completed 2,402 Security Risk Assessments on individuals who work with, possess, or transport select agents and toxins as part of their professional responsibilities and 233 Intelligence Reports that include intelligence notes, analysis of firearm denials, country briefings, and threat assessments.
- Deployed the third increment of the Law Enforcement National Data Exchange, which provided an "internet-type" search interface and a faster search response time.
- Released three officer safety reports through the Law Enforcement Officer Killed and Assaulted (LEOKA) Program: T*hreat Recognition: A Problem for Our Nation's Law Enforcement; Ambushes of Law Enforcement Officers are on the Rise;* and *Law Enforcement Accidental Deaths Steadily Increase*.
- Linked to additional services through the Law Enforcement Online network, including an Intelink search portal, which connects to other secure networks to enhance information and intelligence.

The CJIS Division continued to enhance its biometric identification programs in 2011. With the incorporation of the Next Generation Identification Program's Advanced Fingerprint Identification Technology into the 10-year-old IAFIS system, the accuracy of fingerprint searches increased from 92.0 to 99.6 percent.

Other achievements included the development of innovative biometric technologies with the assistance of the Biometric Center of Excellence (BCOE). In FY 2011, the BCOE sponsored 24 applied biometric research projects concerning fingerprints, deoxyribonucleic acid (DNA), face, voice, and multimodal recognition. Also, through CJIS interoperability initiatives, the Department of Homeland Security and the Department of State have conducted more than 93.1 million searches of IAFIS via IDENT from June 2007 through September 30, 2011.

The Division's campus also continued to grow in FY 2011 with the ongoing construction of the Biometrics Technology Center (BTC), scheduled to be completed in late spring 2014. The BTC will provide additional space for the CJIS Division to accomplish needed biometrics services; house the FBI's BCOE that will provide training, conference space, office and developmental facilities; and accommodate joint biometric research and development efforts between the FBI and the Department of Defense (DoD). The BTC will be comprised of a main building consisting of 400,000 square feet of the CJIS Division space and 60,000 square feet of DoD space.

Prior to FBI Director Robert S. Mueller, III, appointing me as Assistant Director of the CJIS Division earlier this year, I had previously served in executive leadership positions at the CJIS Division from August 2005 through December 2007 when I left to be Special Agent in Charge of the FBI's El Paso Division. From my experience at the CJIS Division, and throughout my career in the field, I have seen how the work that CJIS Division employees do helps to get justice for victims' families. And being able to tell a family you are able to bring about justice for their loved one is like no other experience.

At the CJIS Division, we never forget that our best successes are fueled by our collaboration with our partners. The results of this collective effort help us all to leverage the crime-fighting resources and technological advances we have to better protect our citizens and support those on the front lines of law enforcement and national security.

The **MISSION** of the CJIS Division is to equip our law enforcement, national security, and intelligence community partners with the criminal justice information they need to protect the United States while preserving civil liberties.

The **VISION** is to safeguard our Nation as the global leader in delivering emerging capabilities that empower our partners to connect, identify, and know.

Our **GOAL** is to manage more information and process it faster providing accurate and complete data while maintaining the preservation of civil liberties and purveying additional value-added services.

CONNECT

IDENTIFY

KNOW

Information on-the-spot

Providing cops on the street with facts they need when they need them

On July 29, 2011, the **National Crime Information Center (NCIC)** processed nearly 9.8 million transactions, breaking the previous single-day record for processing by more than half a million transactions. The NCIC is a vital tool that makes available more than 11.7 million active records in 19 centralized files. The files include information on wanted, missing, and unidentified persons and stolen property and are accessed by 92,000+ law enforcement and other authorized criminal justice users. That's a long way from the 95,000 records and five files on wanted criminals and stolen property that started the system in January 1967.

In addition to the information available for immediate query in the NCIC, law enforcement personnel can also avail themselves of some of the other services the system offers, such as providing extracts of vehicle information through the NCIC License Plate Reader (LPR) project. Expanded in 2011, the LPR project supplies vehicle information from the Vehicle, License Plate, and persons files to participating agencies. In turn, the agencies use mobile LPRs to acquire the license plates of parked and moving cars within their jurisdictions and run them against the NCIC extract to fight motor vehicle theft. Agencies participating in the LPR project in 2011 reported more than 1,000 stolen vehicles were recovered with a value of more than $6.5 million. These agencies also credited the LPR data with helping them locate more than 800 wanted persons and 19 missing persons. Currently, law enforcement agencies from 46 states and the District of Columbia participate in the project.

The FBI manages the NCIC system and works in concert with law enforcement to meet law enforcement's ever-changing needs. As such, the NCIC is working toward creating the ability to:

- Add a flagging mechanism to indicate multiple warrants for the same individual by the same Originating Agency Identifier (i.e., ORI) in the NCIC Wanted Person File.
- Add an ethnicity field in the NCIC person records.

NCIC in Action

On February 25, a U.S. Marshal in Pennsylvania contacted the NCIC staff at CJIS for assistance. A 4-year-old child had been kidnapped in Pennsylvania by a non-custodial parent who had threatened to shoot the child and herself if law enforcement interfered. The marshal believed that the suspect was traveling to Florida. He also discovered that there was a New Jersey license plate associated with the suspect's vehicle, but it was not entered in the NCIC record. Therefore, the marshal requested an off-line search for any activity on the license plate.

The off-line search revealed that the license plate had been inquired upon during a traffic stop in Utah on February 19. The marshal in Pennsylvania notified the U.S. Marshals Service in Utah of the situation. Marshals there were able to locate the car at the home of one of the suspect's relatives and place a tracking device on the vehicle. The marshals then followed the vehicle to a gas station as the suspect was leaving town. When the suspect went inside to pay, the marshals safely recovered the child. A loaded gun was subsequently found in the car.

The NCIC off-line search capability produced an investigative lead that ultimately resulted in the safe recovery of the child and the apprehension of the suspect.

Accomplishments

- The NCIC Protective Interest File (PIF) became operational in 2011. The PIF contains records of individuals for whom an authorized agency reasonably believes may pose a threat to the physical safety of protectees or their immediate families. The PIF expanded upon and replaced the U.S. Secret Service Protective File, which was created in 1983.
- The Person with Information (PWI) capability was added to the NCIC Missing Person File. The PWI allows additional searchable information to be appended to a missing person record to assist in locating missing persons.
- The NCIC Mobile Program continued to expand, enabling all FBI agents and U.S. Marshals to conduct inquiries of the NCIC and the Departments of Motor Vehicles using wireless devices through the Law Enforcement Online system.

Quick Facts

- In FY 2011, the NCIC processed an average of **7.9 million** transactions per day—nearly **2.7 billion** total transactions.
- The NCIC's average response time per transaction was **0.0476** seconds.
- At the end of FY 2011, there were **11.7 million** active records in the NCIC system.

Keeping gun sales in check

Promoting the collection and sharing of electronic records to ensure accurate eligibility decisions

One of the primary goals of the **National Instant Criminal Background Check System (NICS)** Section in 2011 was sharing important information that assists states applying for grant funding under the NICS Improvement Amendments Act of 2007. Representatives of the NICS Section met with representatives from 22 states and Washington, D.C., regarding the importance of making information electronically available to the NICS for the NICS Index. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Bureau of Justice Statistics, the National Consortium for Justice Information and Statistics (SEARCH), the National Center for State Courts, and the Department of Justice (DOJ) also attended this important conference.

FEDERAL BUREAU OF INVESTIGATION
NATIONAL INSTANT CRIMINAL BACKGROUND CHECK SYSTEM

In addition, the NICS Section recently began educating the states about an upcoming change to electronic records sharing, securing dates for internal training, and identifying steps needed to make the transition successful. Historically, the NICS Index has contained only information regarding individuals determined to be federally prohibited from possessing or receiving firearms. Beginning in April 2012, the NICS Index will also contain information on individuals possessing “state” firearm prohibitions and/or state permit prohibitions. These entries will automatically respond to a firearm background check based on state of purchase, state of residence, and type of check being performed.

The FBI developed the NICS as a result of the Brady Handgun Violence Prevention Act of 1993 (Brady Act). The Brady Act requires Federal Firearms Licensees (FFL) to request background checks on individuals attempting to receive a firearm. The NICS, launched 13 years ago, ensures the timely transfer of firearms to eligible gun buyers and prevents the transfer of firearms to those prohibited, through a cooperative effort with local and state law enforcement agencies, the ATF, and the DOJ. The NICS also enables FFLs to request an immediate determination as to whether the receipt of a firearm by a prospective gun buyer would violate state or federal law.

The NICS automatically searches more than 70 million records contained in three databases (the National Crime Information Center [NCIC], the Interstate Identification Index [III], and the NICS Index) when authorized gun dealers or FFLs request a NICS check. These records include wanted persons, subjects of protective/restraining orders, and other persons prohibited from receiving or possessing firearms. If an applicant’s name and descriptive information match any records in the databases, the NICS staff and/or state agencies perform further research to determine the eligibility of the applicant.

NICS in action

In May, a delayed transaction prompted a NICS legal instruments examiner to further research a response received while conducting a background check. A Texas State criminal history record contained no firearm disqualifications; however, the record listed the subject as deceased. The NICS examiner, who knew how criminal history records were managed in Texas, knew an individual could be reported deceased in that state with fingerprint verification. The NICS examiner contacted the Texas Department of Public Safety, which determined it did not have the subject’s fingerprints from a coroner’s office. The NICS examiner contacted several law enforcement and court agencies and found that a clerical error had led to an incorrect death notice being placed in the subject’s criminal history record. On May 16, the NICS examiner worked with the agencies holding criminal history records associated with the subject to update the information in the databases to reflect the most current and accurate data, including the removal of the death notice. After the records were modified, the NICS Section contacted the FFL to provide a final status to the transaction, which allowed the buyer to purchase the firearm.

Accomplishments

- NICS conducted more than 14 million background checks in FY 2011.
- The NICS Section exceeded its mandate of an immediate determination rate (eligibility determinations made while an FFL is on the telephone) of 90 percent with a rate of 91.37 percent.
- 100 percent of all the NICS delayed transactions based on the name check search were reviewed within 3 business days.

Quick Facts

- NICS conducted **14,649,784** background checks for gun transfers.
- NICS had **64,330** gun transfers denied federally, keeping firearms out of the hands of felons, fugitives, and other prohibited persons. Since its inception, NICS has issued a total of 862,602 federal denials.
- During each NICS background check, more than **70 million** records are searched.

National information sharing is mission critical to public safety, and the **Law Enforcement National Data Exchange (N-DEx)** provides the criminal justice community with a secure, online national information sharing system with incident, arrest, booking, incarceration, probation, and parole report data. This powerful investigative tool helps criminal justice agencies combat crime and terrorism through the secure collection and processing of criminal justice data from participating agencies' records management systems.

The N-DEx is the result of collaboration among local, county, state, tribal, and federal criminal justice communities. The N-DEx can provide missing links in a case and create partnerships that lead to more effective investigations. These investigations can help disrupt and apprehend individuals and organizations responsible for criminal activities and national security threats.

Increment 3 of the N-DEx, which was deployed March 17, provides users with results in a format similar to that of a commercial search engine. In an era when information sharing is a critical mandate across the criminal justice community, the N-DEx system is well positioned and ready to efficiently and effectively serve criminal justice agencies for decades to come as a national information sharing system.

N-DEx IN ACTION

The N-DEx recently helped enhance officer safety and awareness while protecting a woman and her children during the arrest of a homicide suspect. According to FBI Philadelphia sources, a suspect and two co-conspirators allegedly conducted a home invasion in Philadelphia, Pennsylvania, in the spring of 2008. During the home invasion, the owner of the residence was shot and killed. A suspect from the homicide was identified as one of the defendants in a subsequent Philadelphia Police Department investigation, and an arrest warrant was issued in the summer of 2011. The FBI Philadelphia Violent Crimes Squad assisted in the investigation, and the name of the suspect was queried in N-DEx for additional information. The N-DEx results indicated that the Wilmington, Delaware, Police Department had contact with the suspect in 2010 regarding a domestic abuse case. This information corroborated a possible home address for the suspect. It also noted the possible presence of his wife and two small children. The possibility that children might be present during the execution of the arrest warrant was relayed to case agents in the Philadelphia Police Department, the Wilmington Police Department, and the FBI Wilmington Resident Agency. A SWAT team executed the warrant, and the suspect was arrested without incident in Wilmington, Delaware.

ACCOMPLISHMENTS

- N-DEx Increment 3 was deployed and provides a more intuitive user interface with an "internet-type" search. This increment reduced search response time by over 85 percent.
- Improvements to the Collaboration section make it easier for users to share files, work on documents, and discuss issues.
- In addition to the incident and case reports, arrest, incarceration and booking data contained in the previous increments, the N-DEx can now handle more than 200 million records and accept probation and parole data.
- The N-DEx Program Office was recognized by the Armed Forces Communications and Electronics Association, Bethesda Chapter with a Government-wide Initiatives Excellence Award for Outstanding Achievement for Law Enforcement.
- The N-DEx Program Office was presented with the Integrated Justice Information Systems Institute's Third Annual Innovation Award at the National Forum on Criminal Justice and Public Safety.

QUICK FACTS

- There are over **118 million** searchable records in N-DEx.
- There are more than **720 million** entities (persons, places, things, and events) in N-DEx.
- There are over **5,900** registered N-DEx users (via Law Enforcement Online).
- There are more than **18,300** remote users of N-DEx.
- Over **4,100** agencies contribute data to N-DEx.

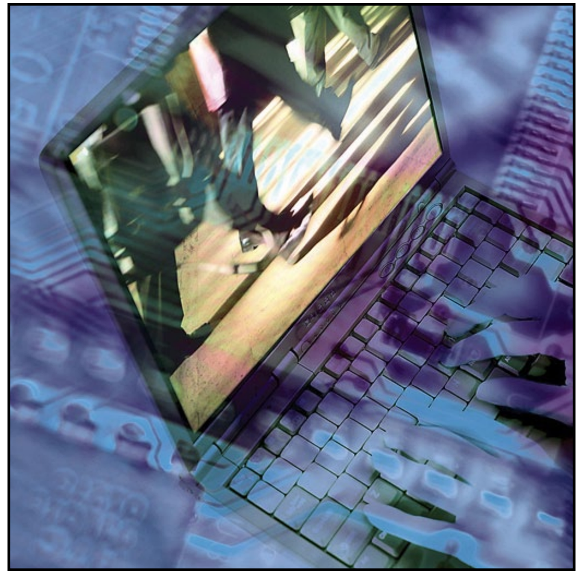
To obtain access to the N-DEx system, law enforcement personnel can log on to www.leo.gov, establish a LEO account, and request membership in the N-DEx Special Interest Group.

In 2011, the **CJIS Division Intelligence Group (CDIG)** expanded the ability of authorized foreign countries to query the National Crime Information Center (NCIC) Vehicle File through a capability known as the NCIC International Cooperative Exchange (NICE). Currently, 43 countries are participating in the NICE, and the CDIG is expanding access to all 184 authorized INTERPOL-member countries.

The FBI, working with the United States National Central Bureau, allows authorized INTERPOL countries to query the NCIC Vehicle File via the NICE. This capability is important because motor vehicles stolen or legally or illegally exported from the United States have been linked to numerous vehicle-borne improvised explosive devices in Afghanistan, Iraq, and Saudi Arabia, as well as to cases of drug smuggling and human trafficking.

In Fiscal Year 2011, the NICE generated more than 483,000 queries that resulted in more than 3,000 hits.

In the future, the NICE will expand to give participating countries access to NCIC person and property files, which are vital to law enforcement worldwide in identifying wanted and missing persons, locating international kidnapping victims, and impeding the ability of sex offenders from traveling undetected in foreign countries. The NICE will substantially increase leads and intelligence information from previously untapped resources for the global law enforcement community and the national security of the United States.



The CDIG also provides tactical intelligence to FBI Field Intelligence Groups; other intelligence community agencies; and local, state, and federal law enforcement organizations to promote public safety and prevent terrorism. The CDIG staff uses multiple databases to conduct checks, known as Security Risk Assessments (SRAs), on individuals who wish to possess, use, or transport biological agents or toxins. The CDIG's mission is to meet current and emerging national security and criminal threats while serving all law enforcement agencies. The CDIG provides its expertise in understanding CJIS systems information to ensure that data are analyzed to their full potential.

CDIG IN ACTION

In March, an individual who was approved to possess, use, or transport biological select agents and/or toxins was arrested and jailed for Abusing a Child, Intent to Torture, Cruel Beating, Inhumane Punishment, and other related charges. The arrest triggered a notification to the Bioterrorism Risk Assessment Group (BRAG) personnel in the CDIG, who researched the case. The Kansas City District Attorney advised that the individual was awaiting a preliminary hearing. If found guilty, the person could receive a sentence of 31 to 136 months in prison. Because the individual was under indictment, the CDIG recommended that the individual's access to biological select agents and toxins be restricted.

While developing data for the CDIG's monthly intelligence notes, analysts discovered an anomaly in firearm denials for Oregon. From November 2010 through January 2011, there were 1,175 firearm denials in Oregon, 294 of which were multiple denials of 98 individuals (25 percent). Based upon monthly reviews of the data, the CDIG staff determined that the percentage was rather high given the time period. The CDIG documented its findings and shared the information with the CJIS Audit Unit and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

ACCOMPLISHMENTS

- In 2011, the CDIG established biometric interoperability capabilities with the Department of Homeland Security (DHS) and the Department of Defense (DoD) to conduct additional search procedures of the DHS's Automated Biometric Identification System (IDENT) and the DoD's Automated Biometric Identification System (ABIS). Previously, the sole source of information for the BRAG staff was the IAFIS. Now, the BRAG staff can also receive information from the IDENT and the ABIS. This provides BRAG personnel with more information than a criminal history check alone. In addition, the IDENT and ABIS furnish information from overseas. The results from these searches can help to determine if the subject's biometrics are associated with a DHS immigration violator case or if the biometrics are associated with a terrorist act that the DoD is investigating.
- The CDIG also developed a pilot program to continuously evaluate the subjects of SRAs via the DHS's IDENT, which helps to protect the Nation against biological threats.
- The CDIG increased the frequency of SRA rechecks from 5 years to 3 years. By decreasing the time between SRA checks, the CDIG further assists national security by giving the bioterrorism prevention community more up-to-date information on those persons with access to biological toxins.
- The CDIG received approval from the FBI Directorate of Intelligence to directly disseminate raw intelligence information reports to U.S. intelligence agencies. Previously, the CDIG had to route intelligence data through another division, which slowed the dissemination process.

QUICK FACTS

- Completed **2,402** Security Risk Assessments on individuals who work with, possess, or transport select agents and toxins as part of their professional responsibilities.
- Produced **713** e-mail notifications, mapping requests, Biometric Verification Reports, and electronic communications that have been disseminated to local, state, and federal law enforcement agencies.
- Produced **233** Intelligence Reports that include intelligence notes, firearm denials, country briefings, and threat assessments.

Online community

Enabling law enforcement collaboration

For 16 years, the **Law Enforcement Online (LEO)** system has provided the criminal justice community with an Internet site for protected communication and the exchange of unclassified but sometimes sensitive information.

With features such as secure e-mail, real-time chat, and forums for questions and answers, LEO facilitates basic communications; it gives access to high-priority messages through the National Alert System. Through LEO, users track state and national dates of interest on the Electronic Calendar and access various types of information via the Special Topic Index. LEO also offers training through eLearning, which supplies topical learning modules and resources.

Beyond the mainstay features, LEO fosters collaboration through Virtual Command Center (VCC) event boards, which are usually short-term, and Special Interest Groups (SIGs), which are often ongoing. For special operations and in national security situations, users initiate VCC event boards to monitor various aspects of an operation that may occur in one location or span several states. The real-time communications of the VCC make critical information immediately available to all of the member authorities that need it, an invaluable tool for the criminal justice community. SIGS are authorized groups of users with specific organizational purposes, e.g., specialized organizations or disciplines in the public safety area. They can be unrestricted (for all users), private (open to members only), or restricted (open only to members who have been granted access).

As part of keeping its users connected, LEO offers a Global Address Book of other LEO members as well as members of the Homeland Security Information Network, the Regional Information Sharing System, Intelink, and the U.S. Department of Justice systems. LEO also provides access to an Intelink search portal and external connectivity with other secure networks to enhance information and intelligence sharing.

As with any successful system, LEO continues to grow to meet law enforcement's ever-changing needs. Currently, the LEO system is undergoing a technical refresh. Planned improvements include upgraded e-mail, search, and chat capabilities; and a language translation feature. This will also include integration into an enterprise portal environment, which will allow authorized users single sign-on access to a variety of essential investigative systems that contain sensitive but unclassified information or controlled unclassified information.

LEO in Action

The FBI Tucson Field Office in Arizona activated a VCC in the aftermath of a shooting spree at a shopping center that killed U.S. Federal Judge John Roll, and critically injured U.S. Congresswoman, Gabrielle Giffords. Initially used as a crisis management tool, the VCC seamlessly transitioned into an information management system supporting the high-profile investigation in Tucson. The suspect was caught by the Pima County Sheriff's Office, arrested by the FBI, and indicted by a Federal Grand Jury on three counts associated with the deadly shooting spree that killed six and injured 13 others.

Two improvised explosive devices disguised as printer toner cartridges were discovered aboard commercial cargo aircraft bound for the United States. President Barack Obama officially confirmed the incidents were a "credible terrorist threat." To head off any other potential attacks, the FBI Philadelphia Field Office launched a VCC to collect, record, and disseminate information among its law enforcement partners concerning the aircraft landing at the Philadelphia International Airport, particularly the United Parcel Service aircraft.

Accomplishments

In FY 2011, LEO:

- Completed a search connection that gives users access to an Intelink search portal hosted by the Department of Justice.
- Equipped CJIS users with single sign-on capabilities via LEO through the CJIS portal link. The CJIS portal established three identity providers and connected five service providers.
- Shared directories of users and services with the Homeland Security Information Network, Regional Information Sharing System, and Intelink, providing a foundation for an integrated, cross-network set of directories to help users more easily locate individuals.
- Enabled VCC and SIG restricted access, which allows LEO to give users access to only certain areas on LEO, including e-mail capability.
- Created an automatic "change password" pop-up box that is displayed when a new member logs into LEO for the first time or is approaching password expiration.

QUICK FACTS

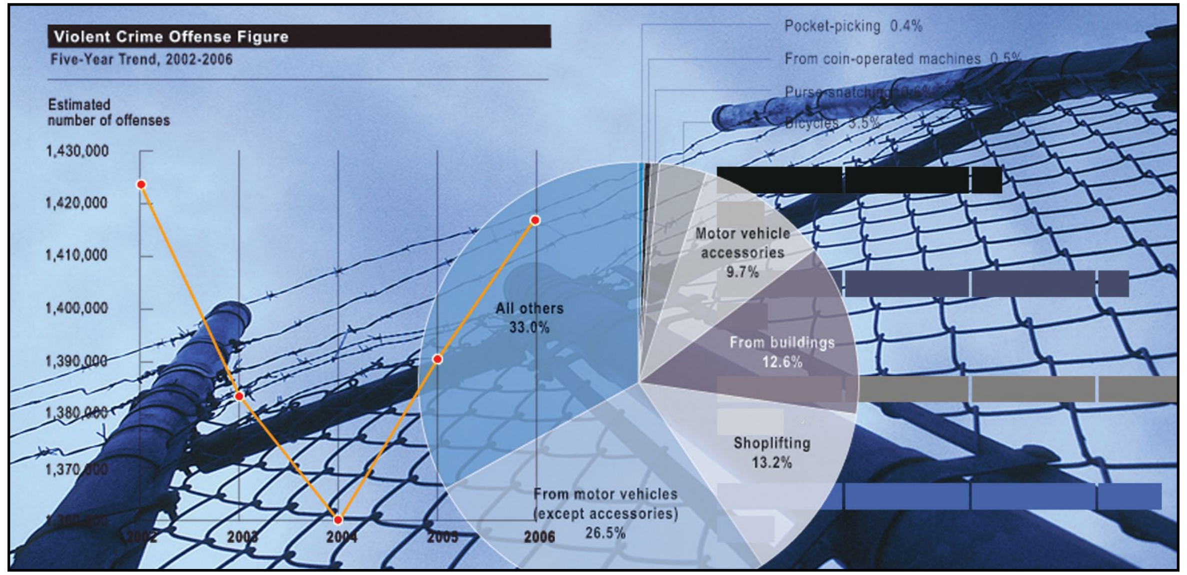
- Law enforcement created **291** Virtual Command Centers and opened **677** VCC event boards in FY 2011. This brings the total of VCCs created on LEO to **1,056**.
- The number of Special Interest Groups created in FY 2011 is **360**. There are now a total of **1,465** LEO SIGs.
- Through LEO SIGs, **50,634** unclassified criminal activity and intelligence documents were shared in FY 2011.

Crunching the numbers

Providing a national perspective of crime

For more than 80 years the **Uniform Crime Reporting (UCR) Program** has effectively done exactly what it was created to do in 1929: provide dependable crime information for use in law enforcement administration, operation, and management. In the process, it has grown and evolved to become a trusted tool for criminologists, government planners, the media, and citizens who want to access a reliable indicator of crime in the United States. With all of those accomplishments, it would be easy for UCR to rest on its laurels. Instead, the Program is in the process of revitalization through a far-reaching redevelopment project to update the Program's outdated technology and boost the timeliness and efficiency of the country's premier crime data collection.

The UCR Redevelopment Project's aim is to reduce, and eventually eliminate entirely, paper submissions and manual entry of data; provide an enhanced external data query tool so data may be viewed, downloaded, and analyzed from the Internet; and decrease the time between data intake and data publication—to provide up-to-date information to users. Working toward its goals, the UCR Program is set to assist contributors in meeting the January 2013 deadline for paperless submission of data.



While in the process of modernization, the UCR Program continued to meet its mission in Fiscal Year 2011 by collecting and validating a variety of crime data from over 18,000 law enforcement agencies and issuing various reports as well as its definitive crime publications: *Crime in the United States, Law Enforcement Officer Killed and Assaulted,* and *Hate Crime Statistics.*

UCR in Action

The UCR Program continues to focus on improving the amount of participation from tribal agencies in Indian country. The number of tribal agencies contributing to the UCR Program was at an all-time high of 183 in Fiscal Year 2011. In addition, the Program is working with the Bureau of Indian Affairs and the Department of Justice's Office of Justice Programs toward an objective of all tribal agencies reporting to UCR in response to the Tribal Crime Law and Order Act of 2010. The goal is to eventually have tribal agencies reporting their data via incident-based submissions through the Department of the Interior's Incident Management and Reporting System, or IMARS.

Mandated to collect Human Trafficking crime by the William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, the UCR Program is working diligently to make sure that training and capabilities are in place to meet the January 2013 target to begin collecting data. Statistics will be collected on both trafficking offenses of Human Trafficking/Commercial Sex Acts and Human Trafficking/Involuntary Servitude.

Accomplishments

- In FY 2011, the UCR Program again provided vital officer safety training classes as part of its Law Enforcement Officer Killed and Assaulted (LEOKA) Program. LEOKA trainers traveled nationally and internationally to bring safety training to officers who daily are in harm's way. In addition, the Program released three officer safety reports: *Threat Recognition: A Problem for Our Nation's Law Enforcement; Ambushes of Law Enforcement Officers Are on the Rise;* and *Law Enforcement Accidental Deaths Steadily Increase.*

- The 2010 editions of *Crime in the United States, Law Enforcement Officers Killed and Assaulted,* and *Hate Crime Statistics* were published on schedule to the Web at www.fbi.gov/about-us/cjis/ucr. Also, 2010 data were added to the interactive, queriable database—UCR Datatool—at www.ucrdatatool.gov.

Quick Facts

- The UCR Program reported that there were an estimated **1.24 million** violent crimes in the United States in 2011.

- There were approximately **1.14 million** "hits" to the UCR homepage on www.fbi.gov in FY 2011.

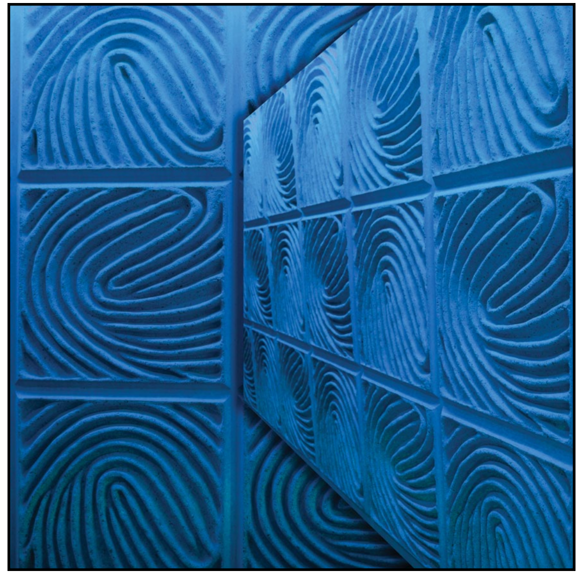
- There were **7,699** criminal offenses reported to the UCR Program as hate crimes.

Automated identification

The world's largest criminal database of fingerprints and criminal history just got better

In 2011, the CJIS Division upgraded the **Integrated Automated Fingerprint Identification System (IAFIS)**, the world's largest repository of biometric-supported criminal history information, with the Advanced Fingerprint Identification Technology (AFIT). The new AFIT enhancement, to the 10-year-old system, increased the accuracy rate to 99.6 percent and improved IAFIS criminal and civil response times. With the AFIT, the average response time for a criminal fingerprint submission is 6-7 minutes; the average response time for a civil fingerprint submission is 54 minutes. The enhancement provides more efficient processing of flat fingerprint impressions for authorized noncriminal justice purposes and improves latent processing services. The deployment of AFIT was virtually transparent to FBI customers.

The IAFIS provides law enforcement with access to specialized files for identification of known criminals through fingerprint identification and for investigative purposes through name-based inquiries. It accesses criminal history record information for noncriminal justice, or civil submissions, such as those individuals being screened for employment or licensing. This helps protect our children, our communities, and our Nation from criminal and terroristic threats.



The IAFIS relies on biographic, fingerprint, and/or criminal history data on file to identify an individual. When a rolled or flat ten-print submission is received, the IAFIS accesses more than 70.2 million criminal fingerprints, 31.7 million civil fingerprints, and 486,000 unidentified latent fingerprints (those left behind at crime/terrorism scenes) to look for a match. If a match is found, the submission goes through the IAFIS Interstate Identification Index (III) segment to access biographic and criminal history information. Finally, the IAFIS delivers a response to the requesting agency on whether a match was found. The III receives an average of nearly 20.5 million name-based inquiries each month for criminal justice and authorized noncriminal justice purposes.

Also in 2011, the CJIS Division began providing Direct Latent Connectivity to the IAFIS for authorized contributors of latent fingerprints that did not have latent search capability through their states. CJIS also made significant upgrades to the Universal Latent Workstation software. The average number of daily latent investigative searches in Fiscal Year 2011 was 597. Progress continues toward a National Palmprint System that will contain palmprint and supplement images suitable for searching within the Next Generation Identification IAFIS, scheduled to become functional in 2013. More than 2.8 million palmprint and supplemental fingerprint images are maintained in this repository, which grew by an average of 1,900 new submissions per day.

More than 18,000 local, state, tribal, federal, and international partners electronically submit requests to the IAFIS, which operates 24 hours a day, 365 days a year. The IAFIS is supported by more than 900 employees providing services focusing on fingerprint comparison, criminal history maintenance, and various other functions.

IAFIS in action

In June, IAFIS helped identify James "Whitey" Bulger, an FBI Top Ten fugitive who had spent 16 years on the run. Bulger was wanted by the Boston Field Office for Homicide, 18 counts of Murder, Extortion, Racketeering, Distribution of Narcotics, and Money Laundering. He was also wanted by the FBI in Tulsa, Oklahoma, for Homicide. At 2:21 p.m. on June 23, 2011, the Los Angeles Field Office submitted fingerprints from Bulger. At 3:42 p.m., fingerprints were received for Bulger's longtime girlfriend Catherine Greig. The IAFIS identified both individuals.

In March, the IAFIS helped identify two suspects, each of whom was wanted for more than 34 years. On March 20 the IAFIS received an electronic fingerprint submission from the sheriff's office in Pine Bluff, Arkansas, for failure to appear. Within minutes, the IAFIS identified the individual as wanted since December 1974 by the sheriff's office in Norwalk, California, for assault with other arrests for Grand Theft Auto, Warrant-Fail to Appear, Kidnapping, Robbery, and Criminal Contempt. Then on March 28, fingerprints of the second subject were received from the sheriff's office in Spokane, Washington. Within minutes, the IAFIS identified the subject as wanted since September 1976 by the sheriff's office in Norwalk, California, for Burglary. The second subject also had previous arrests in California, Hawaii, and Washington, for Hit-and-Run Property Damage, Under the Influence of Narcotic, Burglary, Petty Theft, Possession of Marijuana, Promoting Dangerous Drugs, Possession of Stolen Property, Assault, Obstructing a Law Enforcement Officer, and Taking Motor Vehicle.

Accomplishments

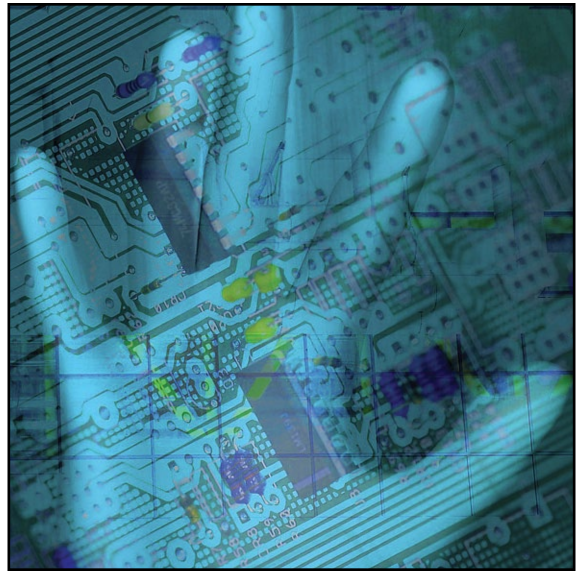
- Average daily fingerprint submissions rose from 42,203 in FY 1999 to 139,138 in FY 2011. Average daily responses increased from 34,728 in FY 1999 to 139,125. For FY 2011, IAFIS receipts at 50,785,515 nearly doubled from FY 2007 receipts of 26,061,552.
- In FY 2011, IAFIS criminal submissions were processed in an average of 9 minutes, 56 seconds, and IAFIS noncriminal/civil submissions in an average of 1 hour, 4 minutes, and 32 seconds.
- More than 70.2 million criminal history records were maintained, which grew an average of 8,000 to 10,000 new identities per day.
- The III received more than 245.4 million name-based transactions in FY 2011.

Quick Facts

- IAFIS identified **307,398** fugitives in FY 2011.
- There are identification data for **570,791** sex offenders in IAFIS.
- The **350 millionth** IAFIS transaction occurred on August 15, 2011.

The first increment of the **Next Generation Identification (NGI) System**, which was deployed in February, marked the first phase in replacing the FBI's Integrated Automated Fingerprint Identification System (IAFIS). The Advanced Fingerprint Identification Technology (AFIT), which replaced the existing Automated Fingerprint Identification System (AFIS), has improved search accuracy to 99.6 percent while adding enhanced processing speed, automation, and flat-print searching.

The NGI has been developed in collaboration with local, state, and federal partners through the CJIS Division's shared management approach to accommodate the increased information sharing and processing needs. The CJIS Advisory Process and The National Crime Prevention and Privacy Compact Council have been instrumental in establishing business processes, policy, privacy considerations, and best practices for NGI services. With full operational capability scheduled for 2014, significant achievements have continued in the NGI development this year.



In August 2011, the CJIS Division nationally deployed the Repository for Individuals of Special Concern (RISC). With RISC, the System allows an officer with a mobile hand-held device to capture and submit fingerprint images of an individual at the scene or on the street. Advanced fingerprint matching software performs a search to compare this fingerprint against the fingerprints of wanted persons, known or appropriately suspected terrorists, Sex Offender Registry subjects, and other persons of special interest.

The NGI System provides automated fingerprint and latent search capabilities, electronic image storage, and electronic exchange of fingerprints to more than 18,000 law enforcement agencies and other authorized criminal justice partners 24 hours a day, 365 days a year.

The NGI Program is in the process of planning enhanced latent search functionality and a National Palmprint System for deployment in 2012 with NGI Increment 3.

NGI in Action

In August, a Florida state trooper conducted a routine traffic stop near Ormond Beach when he witnessed a vehicle being driven with its headlights off. When the trooper approached the car, he smelled marijuana. Following protocol, the trooper asked the driver for his license. As the driver gave the trooper a South Carolina license, the alert trooper noticed the driver had a bank card bearing a different name.

Using a rapid identification (ID) device, the trooper submitted a rapid ID transaction that searched the Florida state system and was also sent to the RISC. The FBI's RISC system returned a "red" response within 46 seconds, notifying the trooper of an outstanding warrant for the subject within the National Crime Information Center (NCIC). The driver was wanted by the Gwinnett County Sheriff's Office in Georgia in connection with a murder and aggravated assault. The warrant had been outstanding for 8 years.

With the RISC, law enforcement agencies across the country now have the ability to use mobile ID devices to rapidly search a national database consisting of the "worst-of-the-worst," enhancing homeland and hometown security.

Accomplishments

- Accuracy in fingerprint searches increased from 92.0 to 99.6 percent with the deployment of NGI's Increment 1.
- The second annual NGI User's Conference, with over 200 in attendance, was held in August 2011. Attendees, representing local, state, tribal, and federal agencies, learned about the benefits and advancement of NGI technology.
- Since the national deployment of RISC on August 25, 2011, 7 states representing 375 law enforcement agencies are now searching the FBI's RISC database.

Quick Facts

- During the 5-day parallel run of AFIS and AFIT during the first week of the NGI Initial Operational Capability (IOC) deployment, AFIT identified, **910** additional candidates as possible matches to submissions.
- There were **1.273 billion** images re-characterized for use within the AFIT in an 8-week timeframe with the IOC deployment.

Partnering to Identify

Collaborating with domestic and international partners to ensure interoperability to identify criminals and terrorists

Biometric Interoperability combines the searching power of the FBI's biometric identification systems with the biometric databases of local, state, national, and international partners, bringing key resources together to identify criminals and terrorists, securing our Nation's streets and borders.

In 2011, advances developed in biometric interoperability through continued information sharing between the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and both the Department of Homeland Security's (DHS's) Automated Biometric Identification System (IDENT) and the Department of Defense's (DoD's) Automated Biometric Identification System (ABIS). With increased access to the IDENT and the ABIS, the FBI has been able to successfully identify and exchange information on criminals who might have otherwise been missed. The search of the full IDENT repository is now available to additional noncriminal justice agencies and programs that use mobile devices to gather biometric information at the scene of an incident or investigation and check it against the FBI's partner databases.

One example of an ongoing interoperability initiative is the FBI's collaboration with the DHS's Immigration and Customs Enforcement (ICE) agency. In April, CJIS Division staff teamed up with ICE to successfully process fingerprint submissions from Panama. ICE agents used mobile devices to submit fingerprints and received responses from the IDENT, the ABIS, and the IAFIS. The ICE agency in Panama is one of 80 agencies taking part in the ICE Biometric Identification Transnational Migration Alert Program.

Biometric Interoperability IN ACTION

On April 22, an individual at George H. W. Bush Houston Intercontinental Airport presented himself as a lawful permanent resident returning with an Alien Registration Card and an El Salvadorian passport. The DHS's Customs and Border Protection (CBP) searched the individual's fingerprints against the IDENT and the IAFIS, which resulted in a referral for a secondary inspection. During the secondary inspection, a positive identification confirmed the subject's extensive criminal history including a 1997 conviction for a crime involving moral turpitude. Because the subject's identity and criminal background was determined, he was refused entry into the United States.

ACCOMPLISHMENTS

- The CJIS Division's Interoperability Initiatives Unit deployed a capability that provides a rapid response of the full IAFIS Criminal Master File. The DHS's Customs and Border Protection began using the rapid response capability at their Primary Inspection locations at the Detroit airport in December 2010 and the Dallas, Atlanta, and Houston airports in 2011. The DHS will expand this capability to additional airports throughout Fiscal Year 2012 to maximize national security at our ports of entry.
- Checks conducted by the Coast Guard on crew members of vessels carrying liquid natural gas and checks conducted by ICE's Biometric Identification Transnational Migration Alert Program can now be forwarded through ABIS to IAFIS for search of the IDENT.
- Searches in support of the IDENT/IAFIS Interoperability grew to 43 participating states and one U.S. territory.

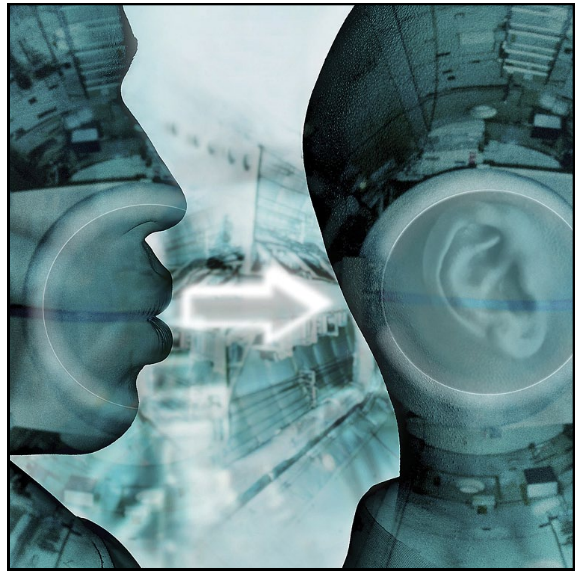
QUICK FACTS

- More than **14.5 million** IAFIS searches were sent to IDENT from October 28, 2008, through September 30, 2011.
- The DHS and the Department of State (DOS) conducted more than **93.1 million** searches of IAFIS via IDENT from June 1, 2007, through September 30, 2011.
- The DHS and DOS searches of IAFIS records resulted in more than **867,705** positive identifications from June 1, 2007, through September 30, 2011.

The **Biometric Center of Excellence (BCOE)** continues to explore and advance new and enhanced biometric technologies, standards, and policies to improve capabilities and expand the use of biometrics to fight crime and terrorism. In 2011, the BCOE sponsored 24 applied biometric research projects concerning fingerprints, deoxyribonucleic acid (DNA), face, voice, and multimodal recognition. One of the projects, the Automated Face Detection and Recognition (AFDAR) prototype, is a forensic image analysis tool designed to allow users to search image datasets by grouping image files based on facial appearance. Image files are loaded into the application, which scans the images for faces, then clusters the faces based on similarities. AFDAR improves the ability of investigative agencies to analyze large collections of images and videos.

Recent technological advances, sponsored by the BCOE in collaboration with agency partners, are now being employed in the development of portable Rapid DNA machines that identify individuals by their DNA. The machines are being designed for use by law enforcement in booking stations to conduct DNA analysis of arrestees more expeditiously than in the past. The machine also has applications for soldiers to identify detainees in the field and for immigration and border agencies to confirm individual identifications or claims of family relationships.

The BCOE also initiated the TattooID Pilot with its partners in the FBI's Laboratory Division.



The TattooID prototype will enable a user to initiate searches using a test image to find similar images. It will also allow a user to enter key words or characters and browse through matching images. The tool is designed to identify individuals by the design and location of their tattoo(s). The pilot program will result in an evaluation of the prototype and identification of any enhancements and future steps needed to deploy the technology.

Along with its many applied research projects, the BCOE continues to partner and support initiatives led by others, as well as sponsor training sessions, meetings, and conferences where leaders from various entities can collaborate to advance biometrics. During one collaborative opportunity, the BCOE supported President Barack Obama's White House Innovation and Infrastructure Initiative by sharing the algorithms used in the TattooID prototype. One of the goals of this initiative is to develop and deploy a nationwide, interoperable, wireless network for public safety. The FBI's Science and Technology Branch, the BCOE, and their partners see the goal as an opportunity to develop an interoperable network that will allow law enforcement to use wireless mobile devices to access resources, like the TattooID tool.

The BCOE also worked with the Executive Branch's National Science and Technology Council (NSTC) by serving as the primary author to update the *National Biometrics Challenge*. The original report, published in 2006, identified key challenges in advancing biometric development. The 2011 update examines the advances made as government, academia, and the private sector "responded" to the challenge issued in 2006. It further describes some of the complex issues that, 5 years later, have yet to be fully addressed.

Because there are so many ideas and options available to the BCOE, identifying which biometric projects to fund is a considerable responsibility. This year, the BCOE developed a web-based Technology Transfer business process to systematically evaluate projects for adherence to the BCOE's mission and measure the return on investment—another step forward in the goal of putting biometric tools into the hands of FBI stakeholders.

Since 2007, the BCOE has combined the knowledge and experience of staff from the Laboratory Division, the Operational Technology Division (OTD), and the CJIS Division. Representatives from these three FBI Divisions continue to develop partnerships and collaborate with law enforcement, academia, and private industry in the United States and around the world.

ACCOMPLISHMENTS

The BCOE:

- Transitioned the facial searching concept into an operational service. This service allows images to be submitted to a facial examiner who processes and compares the images with numerous facial recognition systems and databases. The results are then provided as investigative lead information.
- Published the first issue of the *BCOE Biometric Quarterly*, an internal newsletter providing FBI agents with news and updates about biometric technologies, prototypes, and services.
- Developed training, including Introduction to Biometrics Computer-Based Training; Facial Comparison and Identification Training; and Quick Capture Platform (QCP) Just-in-Time Training, which teaches users to set up and use QCP equipment, as well as troubleshoot common problems.
- Issued the Biometric Investment Policy that requires all FBI entities proposing new investments of more than $25,000 to receive approval from the STB's Biometric Investment Committee.

QUICK FACTS

- The BCOE sponsored **24** applied biometric research projects: 14 with federal agencies (such as the National Institute of Standards and Technology, the Department of Defense, and the Department of Homeland Security) and 10 with academia.
- The BCOE sponsored **20** collaborative events with U.S. government agencies, industries, state and local agencies, and international law enforcement.
- BCOE-developed training was provided to **104** people.

During 2011, the CJIS Division's global **Collections Program** had a significant increase in Flyaway missions and expanded the use of Quick Capture Platforms (QCPs) in the field through the Biometric Identification Tools (B-iD) Program. It also forged more partnerships through the Foreign Biometric Exchange (FBE), working to obtain biometric records and related information for analysis and comparison within the FBI's Integrated Automated Fingerprint Identification System (IAFIS). Through these and other initiatives, the global Collections Program continues to support national and international law enforcement on the biometric front.

With the ability to deploy a team on a domestic or international mission within 4 hours, the **Flyaway Program** assists law enforcement with critical on-site fingerprint identification. In addition to the identification services afforded the agencies requesting these missions, the intelligence gained enhances our national security and border protection.

The **B-iD Program** continues to research new tools to make biometric collections easier and faster. The **QCP**, one of its most prominent tools, delivers the ability to simultaneously query the FBI's IAFIS, the Department of Defense's Automated Biometric Identification System, and the Department of Homeland Security's Automated Biometric Identification System. At approximately 22 pounds, a QCP can be loaded into a backpack. Though developed for the combat arena, QCPs have proven invaluable in gathering biometric information for front-line investigators at home and for other initiatives abroad.

Through the **FBE** missions, CJIS receives and processes biometric inquiries from international sources. No longer limited to fingerprints, FBE missions facilitate the acquisition, review, and analysis of biometric samples and related information from foreign governments and the comparison of them with data from the IAFIS. In addition, CJIS makes similar requests of our partners in foreign countries, i.e., inquiring whether biometric data on U.S. subjects reside in their databases, channeling the requests through the FBI Office of International Operations, Legal Attachés, or the INTERPOL. FBE missions may also include providing training to foreign partners that request it.

Collections in action

In April, a Flyaway team assisted the San Diego Division with "Operation Vise Grip." This operation evolved from earlier gang investigations in north San Diego County. Those investigations revealed that gang members were not only involved in typical gang activities such as drug trafficking, but they were also active in prostituting juvenile females. Most of the subjects arrested were charged under Title 18, USC 1961: Racketeer Influenced and Corrupt Organizations (RICO). A total of 38 subjects from the "Insane Crip Gang," "Deep Valley Crips," and "Crook, Mob, Gangsters" were indicted for alleged sex trafficking of minors and adults, attempted murder, kidnapping, extortion, and the distribution of controlled substances. As part of this investigation, 30 minors, many of them runaways, were rescued.

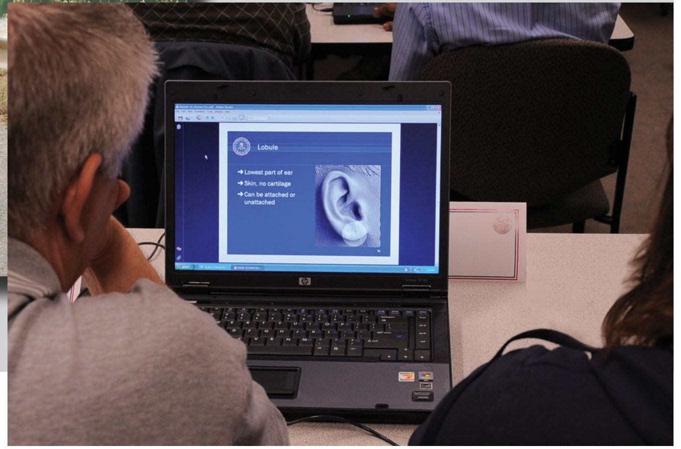
In January, a CJIS team on an FBE mission traveled to Mexico City for an exchange of biometric and biographic information. The CJIS team provided fingerprints belonging to 234 FBI fugitives with violent criminal histories for comparison against the Mexican Automated Fingerprint Identification System. In return, Mexican authorities provided 95 fingerprints related to high-ranking drug cartel members and prison escapees to be run against the FBI's IAFIS. Of the 234 FBI records provided, 42 had been arrested at some time in Mexico. Of the 95 Mexican records provided, 27 matched existing U.S. records. Once the FBE team placed stops on the records from Mexico, U.S. authorities arrested five individuals who were escaped prisoners from Mexico and will be returned. In addition, the FBE mission established a collaborative relationship with the Government of Mexico.

Accomplishments

- Flyaway missions were completed in locations such as Miami, Puerto Rico, New York, Philadelphia, Memphis, Norfolk, and San Diego, resulting in the acquisition of over 1,000 criminal fingerprint, DNA, and photographic samples.
- QCPs were deployed in support of the following initiatives:
  - Crimes Against Children Unit
  - Violent Crimes Squads
  - Hostage Rescue Team
  - Counterterrorism Division's Fly Team
  - SWAT Maritime Teams
  - Southwest Border Initiative Teams
  - International Innocence Lost Task Force
  - CJIS Flyaway missions
- Over 500,000 biometric collections were obtained by FBE missions to countries such as Afghanistan, Iraq, Dominican Republic, El Salvador, Philippines, Indonesia, Somalia, Haiti, Belize, and Yemen.
- The global Collections Program worked with the Department of Homeland Security and the Department of State to sign Preventing and Combating Serious Crime Agreements with 19 foreign partners. This will allow for the automated exchange of biometric information when there is a criminal justice purpose.

Quick facts

- In 2011, **29** Flyaway missions were completed.
- **149** QCPs were deployed operationally.
- CJIS successfully completed **49** biometric exchange missions with foreign governments through the FBE.



A sixteenth century philosopher said ***"Knowledge is power."***
To modern law enforcement, knowledge is that, and more.

The **CJIS Division** gives our law enforcement, national security, and intelligence community partners the power to connect, identify, and, most importantly, to know. CJIS gives them:

The power to know where the danger lies;

The power to know who the person is;

The power to know how the facts connect;

The power to know what the scope of crime is in their area;

The power to know what others know.

CJIS provides the "power to know"—a crucial tool for our partners in fighting crime and terrorism.

The Advisory Process

We partner with law enforcement to fight crime and prevent terrorism

At its June meeting in Kansas City, Missouri, the Criminal Justice Information Services **Advisory Policy Board (APB)** voted to allow all criminal justice agencies access to the Law Enforcement National Data Exchange (N-DEx) for law enforcement investigations, pre-sentencing investigations, supervision investigations, data management, and training.

Access to the N-DEx was one of the far-reaching subjects that the APB, working with our law enforcement partners, considered in 2011. Other topics ranged from changes in the Uniform Crime Reporting Program (UCR) and the National Crime Information Center (NCIC) to updates on the programs at the CJIS Division.

The APB is responsible for reviewing appropriate policy, technical, and operational issues related to CJIS Division programs and for making appropriate recommendations to the Director of the FBI. The Advisory Process is a shared management concept by which law enforcement representing local, state, tribal, and federal system users nationwide provide guidance and direction regarding the systems and initiatives managed for law enforcement by CJIS. This includes nationally known initiatives involving the NCIC, the UCR Program, the Next Generation Identification (NGI), and the N-DEx.

The 34-member APB reviews and discusses all the material and provides final recommendations.

Subcommittees are established to thoroughly review complex policies, issues, program changes, and formulate alternatives and recommendations for the consideration of the entire APB. Within this structure, members divide duties among eight ad hoc subcommittees:

Bylaws—responsible for evaluating proposed changes to the Bylaws for the CJIS Division APB and Working Groups and for recommending appropriate language with proper notice to the APB for approval.

Identification Services—responsible for all projects related to the FBI's fingerprint identification programs/initiatives and the criminal justice use of criminal history information.

Information Sharing—reviews and evaluates the development of the N-DEx Program.

National Crime Information Center—addresses issues related to the NCIC Program.

Public Safety Strategy (PSS)—reviews issues being considered by the various APB Working Groups and subcommittees, topics, programs, and issues being addressed by other law enforcement professional associations/organizations, and current events in the criminal justice and information processing arena.

Sanctions—responsible for evaluating the results of audits conducted of participants in CJIS programs.

Security and Access—responsible for reviewing the hardware and software security policy for current CJIS Division computer systems as well as those systems under development.

Uniform Crime Reporting—responsible for reviewing issues concerning the UCR Program, including the Summary Reporting System, the National Incident-Based Reporting System, Law Enforcement Officers Killed and Assaulted Program, and the Hate Crime Statistics Program.

A variety of task forces, made up of subject matter experts who are called upon to address specific issues, report to the ad hoc subcommittees. The newest task force is the Direct Connect Task Force, which deals with existing and new technological advances relevant to CJIS service connectivity and reports to the PSS. Other task forces include the Joint Task Force on Rap Sheet Standardization, the Disposition Task Force, the Identification Services Collaboration Group, the Information Sharing and N-DEx Operations Task Force, and the Warrant Task Force.

The APB and subcommittees are advised of the recommendations of Working Groups, which make the initial review of operational, policy, and technical issues related to CJIS Division programs. All 50 states, as well as U.S. territories and the Royal Canadian Mounted Police are organized into four Working Groups: North Central, Northeastern, Southern, and Western. Federal agencies participating in CJIS Division programs comprise the Federal Working Group.

Accomplishments

- FBI Director Robert S. Mueller, III endorsed the APB-recommended *CJIS Security Policy.*
- The APB recommended several key NGI requirements including standards development, service level agreements, and latent print processing.
- The APB has approved six new NCIC file sharing initiatives, one new biometric sharing initiative, and endorsed creating a biometric sharing task force to evaluate future biometric requests.

Quick Facts

- Law enforcement agencies nationwide and our CJIS internal subject matter experts submitted **124** potential topics.
- The Division forwarded **101** recommendations related to improving and enhancing our systems and programs to Director Mueller for his review, approval, and implementation.
- Participants researched, prepared, and reviewed **329** staff papers.

The Compact

We partner with policy makers to provide criminal history information for employment/licensing screening

Whether it's a background check for a teacher, a nursing home aid, or a bank teller, it is important that the most accurate and complete information is available and known before a position of trust is offered. If the potential candidate has lived in more than one state, it can be more complicated to locate relevant records. It was determined in the late 1970s that state criminal history records were often more complete than national records. States often have additional arrest and disposition information within the state files, such as District Attorney records and court records. Because states had varying statutes or policies that restricted the dissemination of records for noncriminal justice purposes, a federal law, or Compact, was necessary to facilitate criminal record dissemination between states. The **National Crime Prevention and Privacy Compact Act of 1998 (Compact)** addressed the need to decentralize criminal history record information (CHRI).

The Compact led to the organization of the 15-member Compact Council (Council), which establishes rules and procedures to facilitate the use of CHRI for noncriminal justice purposes, such as screening an individual's suitability for employment, licensing, or placement in positions of trust. The CJIS Division provides mission critical support to the Compact Council and is home to the FBI's Compact Officer. The FBI's Compact Officer is responsible for ensuring that agencies abide by the rules and regulations created by the Compact Council.

The Compact also provided the legal framework for the noncriminal justice use of the FBI's Interstate Identification Index (III) and facilitated complete decentralization of criminal history records. The III is the national repository for sharing national criminal history information and is a major segment of the FBI's Integrated Automated Fingerprint Identification System (IAFIS). The Council monitors the use of the III for noncriminal justice purposes to ensure the protection of an individual's privacy while facilitating the nationwide exchange of automated CHRI.

The Compact has been in effect since April 28, 1999, when it was ratified by two states. Each state that ratifies the Compact gives authority to share its state criminal history record information (on an interstate basis) for all authorized purposes, including fingerprint-based background checks for noncriminal justice reasons. To date, 29 states have ratified the Compact and an additional 11 states have executed a Memorandum of Understanding with the Council as a precursor to ratification.

When the III concept was adopted to decentralize criminal history record-keeping in 1978, the concept's ultimate goal was the National Fingerprint File (NFF). The NFF places the management and responsibility for the effective control, collection, maintenance, and dissemination of state record files solely with the state. An NFF participant is a III-participating state and a Compact signatory that has agreed to provide its criminal history records. Currently, 14 states participate in the NFF.

ACCOMPLISHMENTS

The Compact Council, the FBI's Compact Officer, and staff:

- Provided guidance to the Centers for Medicare and Medicaid Services in their endeavor to launch a national background check program as directed in the Patient Protection and Affordable Care Act of 2010.
- Developed a plan to assist states in achieving NFF implementation in a more timely fashion.
- Developed educational information that may be used as a foundation for advising agencies of their obligations in the background check process and for notifying applicants of their federal privacy rights.

QUICK FACTS

- In FY 2011, nearly **24.3 million** background checks were conducted for screening an individual's suitability for employment, licensing, or placement in positions of trust.
- To date, **29** states have ratified the Compact.
- Of the compact states, **14** are National Fingerprint File participants.

In 2011, the CJIS Division continued to deliver its services quickly and efficiently to its customers. The technology available at CJIS allows our staff to meet the ever-expanding need for rapid response times and increases in processing capacities. CJIS operates the critical systems that daily assist our Nation's efforts to fight crime and support our military efforts—365 days a year.

The CJIS Information Technology (IT) infrastructure provides the technology to support the growth in these vital systems:

The **Integrated Automated Fingerprint Identification System (IAFIS)** continued to see a dramatic rise in fingerprint submissions as 70,000 to 75,000 prints originated daily from Customs and Border Protection and 30,000 prints came daily from the Department of State. The IAFIS averaged 139,138 receipts per day this fiscal year.

The **National Instant Criminal Background Check system (NICS)** completed 14,649,784 FBI background checks in support of firearm sales nationwide. This total was up more than half a million from the 14,088,406 background checks conducted in Fiscal Year 2010.

The **National Crime Information Center (NCIC)** averaged 7.9 million transactions per day in Fiscal Year 2011 and set a new daily record by processing 9,768,568 transactions on July 29. A total of 2,675,230,563 transactions were processed by the NCIC this fiscal year, and the response times averaged 0.0476 seconds.

Despite the great demand for this information, these systems continue to provide results well within their anticipated goals and to exceed the expectations for their availability. Our customers can be sure that, in the future, the CJIS staff will be prepared to deploy whatever technological advances become available to further improve and enhance these services.

Response Times

IAFIS Criminal Fingerprint processing:
Goal 2 Hours; Actual 9 minutes, 56 seconds

IAFIS Noncriminal (Civil) Fingerprint processing:
Goal 24 Hours; Actual 1 hour, 4 minutes, and 32 seconds

NCIC transaction processing:
Goal 2.0 Seconds; Actual 0.0476 seconds

NICS Immediate Determination Rate (IDR):
Goal Greater than 90 percent; Actual 91.37 percent

(Note: The IDR is the percentage of eligibility determinations made without any delays.)

System Availability

IAFIS	Goal 97.5%;	*Actual* 99.0%
NCIC	Goal 99.5%;	*Actual* 99.8%
NICS	Goal 98.0%;	*Actual* 99.8%

(Note: System availability is less than 100% due to scheduled outages for maintenance, which is approximately 1.5 hours per month.)

Our campus

Situated in Clarksburg, West Virginia, on nearly 1,000 rolling acres, the CJIS Division campus includes a Main Building of 500,000 square feet housing offices and a state-of-the-art Data Center that is a hub of activity serving law enforcement across the Nation. Also on site are a Service Center, the Lasting Impressions Child Development Center, the Central Plant, and a Visitor's Center. Looking forward, there is a new addition coming to the CJIS campus as the CJIS Division is partnering with the Department of Defense (DoD) to develop a new Biometrics Technology Center (BTC). This coexistence of the two federal agencies will provide a very unique collaboration between the FBI and the DoD to protect the United States while preserving civil liberties.

For more information about the CJIS Division,
visit: ***www.fbi.gov/about-us/cjis***

Under construction

The BTC is scheduled for completion in late spring 2014 and will house the CJIS Division's Biometric Services Section (BSS) and the DoD's Biometrics Identity Management Agency (BIMA). The new building will serve three purposes: to provide additional space for CJIS to accomplish needed biometrics services in one location on the main CJIS campus; to house the FBI's Biometric Center of Excellence that will provide training, conference space, office and developmental facilities; and to accommodate joint biometric research and development effort between the FBI and the DoD. The BTC will be comprised of a main building consisting of 400,000 square feet of the CJIS Division space (roughly 3/4 the size of the current facility) and 60,000 square feet of DoD space.